SECTION B – SUPPLIES OR SERVICE/PRICES

1.0 CONTRACT TYPE

This is a hybrid type contract with Cost-Plus-Award-Fee (CPAF), Firm-Fixed-Price (FFP), and Cost Reimbursement (CR) contract line items (CLINs)

< LABOR RATES TO BE INCLUDED AT TIME OF AWARD>

2.0 TRAVEL COSTS

All travel will be reimbursed at cost in accordance with the Federal Travel Regulations (FTR). The Contractor shall seek written Government approval (Contracting Officer (CO) or COR) at least two weeks in advance, prior to incurring any costs associated with non-local travel.

Local travel will not be reimbursed within a 50 mile radius of the worksite. As the Contractor may locate personnel outside the Washington D.C. metropolitan area, for purposes of local travel only, the worksite shall be considered the Washington D.C. metropolitan area, or the location of contractor's personnel, whichever is within the 50 mile radius.

The Contractor shall use the federal lodging and per diem allowances in accordance with FAR 31.205-46 and the applicable FTR governing the travel performed directly referable to this contract. The Government will not reimburse transportation costs in excess of coach class commercially scheduled air or ground transportation by the most expeditious route.

Travel reimbursement request must be submitted (in writing) in sufficient time for the Contracting Officer or Contracting Officer Representative to give prior approval, and must identify (i) the name of the traveler, (ii) destination (s) including itinerary, (iii) purpose of the travel, and (iv) cost breakdown.

To be reimbursed, invoices, including travel expenses must include a detailed breakdown of the actual expenditures invoiced.

3.0 MATERIALS/OTHER DIRECT COSTS (ODCs)

The Contractor shall procure material/ODCs when essential to task performance and approved by the Program Manager and the Contracting Officer. ODCs must be approved by the CO prior to incurring any costs. ODCs must be approved by the CO, and must be necessary, allowable, and allocable for performance of this contract. ODCs must be submitted in sufficient time to the CO to give prior approval, and must identify the purpose of the ODCS and provide a detailed cost breakdown. The Contractor shall maintain the original or legible copy of receipts for all ODCs invoiced. The Contractor shall be reimbursed on an actual cost basis.

All materials purchased by the Contractor for the use or on behalf of the Federal Government shall become the property of the Federal Government. The Contractor shall document the transfer of materials in addition to an account of all materials consumed during the performance of the contract. The Contractor shall furnish a copy of such documents at Quarterly Program Management Review Meetings.

(End of Section B)

SECTION C – DESCRIPTION/SPECIFICATIONS

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA)
EMERGENCY COMMUNICATIONS DIVISION (ECD)
PRIORITY TELECOMMUNICATIONS SERVICES (PTS)
PERFORMANCE WORK STATEMENT (PWS)

1.0 PURPOSE

The purpose of this Performance Work Statement (PWS) is to specify the work outcomes required of the Contractor to provide and support communications services at a level that assures a high probability of their availability and performance to meet the needs of authorized National Security and Emergency Preparedness (NS/EP) users under all levels of stress. The Contractor shall provide task/program management, engineering, service agreements acquisition, and operations, administration, maintenance, and provisioning (OAM&P) support for Priority Services (PS). PS consists of legacy Government Emergency Telecommunications Service (GETS), Special Routing Arrangement Service (SRAS), Wireless Priority Service (WPS), and Next Generation Network (NGN) Priority Service (PS). In addition to the services described above, under optional CLINs, when exercised by the Government, the Contractor shall support the planning, implementation and testing of bridging and NGN PS technology refreshment-type changes that will contribute to the continuing viability and effectiveness of the PS as it transitions to NGN. The Contractor shall furnish all personnel, materials, services, and facilities necessary to perform the requirements set forth in this PWS.

2.0 SCOPE

This PWS specifies the outcomes required of the Contractor, to provide carrier service agreements, requisite OAM&P and engineering support for PS and other related priority services. Engineering is required for sustainment and technology refreshment of the specified services to ensure the service capabilities do not degrade, as Public Switched Network (PSN) technology upgrades occur, and that the services continue to be effective under all levels of stress.

3.0 BACKGROUND

The PS program responds to White House tasking to address the communications needs for Continuity of Operations (COOP) and Continuity of Government (COG). Through priority enhancements to the national telecommunications infrastructure, the Emergency Communications Division (ECD) can effectively and economically address the COOP/COG needs while also providing a significant benefit of assured communications during NS/EP incidents to the broader national, state, local, and non-government NS/EP community. PS, by cost-effectively leveraging the PSN, helps to ensure the preparedness of the nation to prevent, respond to, and recover from, threatened and actual domestic terrorist attacks, major disasters, and other emergencies. PS has, and will, continue to support NS/EP users' telecommunications requirements during disasters and emergencies.

4.0 PERIOD OF PERFORMANCE

See Section F – Item 1.0.

5.0 PERFORMANCE OBJECTIVES, GOALS, AND OUTCOMES

Maintaining PS is vital to the Government, including National Leadership, to ensure emergency communications are available to coordinate recovery efforts in responding to disasters and crises, including acts of terrorism and war. In maintaining PS in an all-hazards environment, the OEC requires contractor engineering, acquisition, program management, integration, coordination, and OAM&P support.

The purpose of this PWS is to specify the performance requirements for the Contractor to provide communications services and service support at a level that assures a high probability of their availability to meet the needs of authorized NS/EP communications users under all levels of stress. The Contractor shall provide engineering and planning; implementation, integration, and coordination; communications services and operations, administration, maintenance, and provisioning support as required for existing PS voice services as well as future services support that will ensure NS/EP communications requirements are met through current and next generation communications networks.

This PWS requires the Contractor to arrange for provisioning selected voice capabilities, as well as future services, within carrier networks and to maintain these services through OAM&P activities specified herein, and to engineer, implement, test and maintain NS/EP priority communications services within converging and next generation communications networks.

In acquiring priority service, the Contractor shall be restricted to US owned carriers, service providers, and vendors; unless specifically authorized by the Government to deal with non US owned companies. In recognition that the vast majority of telecom vendors are foreign owned, OEC will streamline its approval process. The Contractor shall be prohibited from contracting for Priority Service with service providers utilizing Chinese manufactured telecommunications equipment for handling NS/EP traffic, unless specifically authorized by the government.

The Contractor shall provide the following support:

(a) Provide and maintain specified wireline and wireless voice service within the carrier subcontractor networks in accordance with NS/EP Priority Services Functional Requirements Specification (FRS) and the Special Routing Arrangement Service (SRAS) FRS, as modified by the respective Requirements Traceability and Verification Matrices (RTVMs) and this PWS.
(b) Provide service evolution planning for the continued enhancement and evolution of NS/EP priority services in conjunction with the evolution of the communications service providers under subcontract.
(c) Provide additional service implementation and OAM&P within the carriers' (specified in section 5.2.) evolving networks and those carriers' interfaces to the networks of other providers of NS/EP Priority Services in order to maintain and enhance NS/EP communications.
(d) Investigate and provide recommendations for other IP based priority data services.

The Contractor shall provide these services with minimal adverse impact upon public communication network facilities, commercial traffic, and Government networks, while minimizing cost and risk to the Government.

The Contractor is encouraged to provide solutions that minimize the number of mechanisms used to achieve a higher probability of call/session establishment from the User Equipment (UE) to the network, and the network to the UE (i.e., end-to-end communications) during times of network stress

(coordination with AT&T, Sprint and Verizon will be required). The Contractor is highly encouraged to reuse technology in order to contribute to minimal service-specific development and subsequent monetary cost. Lastly, in acquiring carrier services, the Contractor shall work to ensure that the investment is protected from service provider upgrades. OEC recognizes that service provider migration to new platforms such as 5G could require added NS/EP investments; however, acquired NS/EP services shall be protected from upgrades/changes to existing platforms. Service providers, when replacing PS enabled network equipment on existing platforms shall be required to enable the new products with equivalent PS features and functions at no additional cost to the Government.

5.1. Contract/Program Management

Contract/Program Management Objective:

The Contractor shall manage the contract through the use of the following:

- Project plan
- Quality Assurance Surveillance Plan (QASP)
- Status meetings with the government
- Status reports to the government

In maintaining nationwide PS coverage and follow-on services, the Contractor shall provide the following support:

- Program and engineering management to ensure that schedule, cost, and performance goals are met
- Planning and coordination to manage PS agreements with service providers
- Establishing processes for quality assurance to include producing the Quality Assurance Surveillance Plan (QASP), and for progress and cost reporting
- Serving on the Service Provider Council, along with T-Mobile, to ensure PS follow-on services are interoperable and to resolve issues that may arise
- Adhering to DHS Certification & Accreditation (C&A) requirements and providing requisite documentation regarding database or other collection of DHS data in order to obtain and maintain full Authority to Operate

5.2. GETS, SRAS, and WPS Services

5.2.1. GETS Service Objective

The Contractor shall sustain GETS and where required SRAS by renewing the requisite service subcontracts to maintain GETS/SRAS priority features and functions within local exchange carriers' (LEC) networks. In order to sustain GETS/SRAS, the Contractor shall establish LEC arrangements to maintain GETS priority features and functions within carrier networks during the base year period, and be prepared to retain the arrangements for all option years.

GETS carrier subcontracts shall include the following:

- GETS features shall be provided on all switches for which the features are available in the software release deployed on the switch

- GETS features shall be configured and maintained in accordance with Contractor provisioning guidelines
- Where Advanced Intelligence Network (AIN) infrastructure is available and Alternate Carrier Routing (ACR) has previously been provided, ACR shall continue to be provided for GETS calls
- GETS Operational Measurement data shall be provided to the Contractor daily from switches with GETS features
- If delivered under the previous carrier service subcontract, call record data shall be continue to be provided to the Contractor monthly for all GETS calls

The Contractor shall establish service agreements expeditiously to ensure no lapse in service.

The Contractor shall present the results of these subcontract negotiations to the OEC in a briefing. Subject to OEC approval, the Contractor shall enter into subcontracts with the LECs for GETS.

After establishing service subcontracts, if all or any portion of the LEC networks specified in section 5.2.1.1 is acquired by another company, the Contractor shall pursue continuation of GETS service with the acquiring company under section 5.6. Technology Refreshment.

5.2.1.1. GETS Carrier Agreements

The Contractor shall subcontract with the LECs shown in Table 1 below. For any Tier I, II, or III LEC required, as shown in Table 1, for which a service arrangement is not in place at the time of contract award, the Contractor shall establish a service arrangement, consistent with arrangements with the other carriers, as a task under section 5.6. Technology Refreshment.

The Contractor shall structure the GETS required LEC agreements as basic work and optional tasking, to reflect the government's objective/desire to pursue alternative direct contracts to acquire specific GETS LEC services. The optional tasks are unilateral options solely at the government's discretion.

Table 1

TIER 1	**TIER 2**	**TIER 3**
CenturyLink (including legacy carrier: tw Telecom)	Cincinnati Bell	Ben Lomand
	Frontier	East Ascension
	Hawaiian Telecom	GTA Teleguam
	Claro	Matanuska
	TDS	Micronesia
		Neutral Tandem
	Windstream	Pioneer Telephone
		Shentel
		Consolidated Communications,Mattoon, IL

		Peerless Network

5.2.1.2. Carrier Agreement Requirements

The Contractor may include the following OAM&P-type requirements for GETS in their carrier agreements.

• **Provisioning Requirements:** Specifies the provisioning of the GETS features, to include parameter settings and routing

• **OA&M Reporting Requirements:** Specifies the GETS operational data that the carrier shall deliver to the Contractor

• **GETS Billing Data Reporting Requirements:** Specifies carrier reporting to the Contractor of GETS completed and billable calls

• **GETS Call Detail Records Reporting Requirements:** Specifies carrier reporting to the Contractor of all GETS call attempts

• **Annual Carrier Reviews:** Specifies the requirements for the carrier to conduct an Annual Program Review including Network Evolution and Roadmap planning for the Contractor and the Government (virtual meetings preferred)

• **Configuration Report Requirements:** Specifies the GETS provisionable parameters that the carrier must audit and verify are provisioned according to the Provisioning Requirements

• **Generic Network Service Verification Test (NSVT) Test Plans and Reports:** Specifies the service verification testing and reporting that the carrier shall perform in coordination with the Contractor to ensure GETS functionality in an operational network

• **Other Network Data:** As specified, other data decided by OEC in the Service Provider Council (SPC) as relevant to determine NGN service performance, including handset data**.**

5.2.2. WPS Service Objective

The Contractor shall **s**ustain WPS by providing the requisite contracting support to maintain WPS priority features and functions within wireless carrier networks. In order to sustain WPS, the Contractor shall make arrangements with wireless carriers to maintain WPS priority features and functions within their networks.

WPS carrier subcontracts shall include the following:

- WPS features shall be provided on all mobile switching centers (MSCs) and radio access networks (RANs) for which the features are available in the software release deployed on the MSCs and RANs.
- WPS features shall be configured and maintained in accordance with provisioning guidelines specified by the Contractor
- WPS operational measurement data shall be provided to the Contractor daily from all network components that generate WPS-specific OMs
- Call record data shall be provided to the Contractor monthly for all WPS calls

The Contractor shall negotiate with the carriers to extend the existing carrier subcontracts as the basis for establishing the new contracts.

After establishing service subcontracts, if all or any portion of the carrier networks is acquired by another company, the Contractor shall pursue continuation of WPS with the acquiring company under section 5.6.Technology Refreshment.

5.2.2.1. WPS Carrier Agreements

WPS required carrier agreements are as follows:

- T-Mobile
- US Cellular
- General Communications Inc. (GCI)
- Cellcom
- C-Spire
- Cellular One

5.2.2.2. Carrier Agreement Requirements

The Contractor shall continue the following OAM&P-type requirements for WPS in their carrier agreements by extending the pre-existing subcontracts which include these requirements. Contractor labor to support these requirements shall be included under section 5.4.

• **Provisioning Requirements:** Specifies the provisioning of the WPS features, to include parameter settings and routing

• **OA&M Reporting Requirements:** Specifies the WPS operational data that the carrier shall deliver to the Contractor

• **Configuration Report Requirements:** Specifies the WPS provisionable parameters that the carrier must audit and verify are provisioned according to the Provisioning Requirements

• **Generic NSVT Test Plans and Reports:** Specifies the service verification testing and reporting that the carrier shall perform in coordination with the Contractor to ensure WPS functionality in an operational network

• **WPS Billing Data Reporting Requirements:** Specifies carrier reporting to the Contractor of WPS completed and billable calls

• **WPS Call Detail Records Reporting Requirements:** Specifies carrier reporting to the Contractor of all WPS call attempts

• **Other Network Data:** As specified, other data decided by OEC in the SPC as relevant to determine 4G and 5G service performance

• **Annual Carrier Reviews:** Specifies the requirements for the carrier to conduct an Annual Program Review including Network Evolution and Roadmap planning for the Contractor and the Government (virtual meetings preferred).

5.3. Engineering Support

5.3.1. Sustainment Engineering

The Contractor shall provide engineering to extend the service viability for GETS and WPS carriers, while ensuring that these services support user requirements in a manner that protects NS/EP equities. The Contractor shall seek to reduce program costs by engineering solutions and negotiating carrier agreements that extend the lifespan of existing priority services. Contractor shall coordinate sustainment engineering, as appropriate, with AT&T, Sprint, and Verizon through the OEC and the SPC.

The Contractor shall include in Carrier Annual Program Reviews a section on future services planning that addresses carrier plans for network and service evolution as they impact sustaining GETS and WPS.

The Contractor shall submit to the Government a monthly White Paper and a briefing that addresses sustainment engineering topics. The Contractor shall coordinate White Paper and briefing topics with the Program Manager.

5.3.1.1 Sustainment Engineering for Interoperability

The Contractor shall provide engineering to maintain GETS interoperability and to maintain WPS interoperability. Contractor's engineering shall maintain interoperability of PS features across the PS feature set and across multiple carriers. The Contractor shall perform actions to remediate interoperability issues that do not incur implementation costs to the OEC. In those instances in which the Contractor recommends remedial actions that may incur costs, the Contractor shall provide the OEC with a decision brief to initiate a Technology Refreshment contract modification.

5.3.1.2 Sustainment Engineering for Performance

The Contractor shall provide engineering to ensure that GETS performance and WPS performance meets the stated objectives. The performance objectives are:

- **GETS:** Enhanced call completion rates for NS/EP users that are greater than what the general public experiences during disaster or crisis with the objective of 90% call completion at eight times busiest hour traffic profile in their network
- **WPS:** Enhanced call completion rates for NS/EP users that are greater than what the general public experiences during disaster or crisis with the objective of 80% call completion at a minimum of twenty times busiest hour traffic profile in their network
  Contractor's performance engineering shall support the Operational Support testing and end-to-end performance metrics (section 5.4.).

5.3.1.3 Monitoring GETS, SRAS, and WPS Viability

The Contractor shall work with all service providers under contract to monitor viability of PS. The Contractor will provide regular reports on carrier plans to transition to IP. Reports should include time schedules for migrating to IP, decommissioning circuits and networks, reduction in existing technology coverage or availability, and any carrier plans that will lead to PS performance degradation.

5.3.1.4 Sustainment Engineering for Viability Extension

The Contractor shall provide GETS and WPS engineering to extend the service viability by analyzing carrier network evolution and technology changes to identify potential impacts to GETS and WPS and to engineer a cost-effective solution, if required. The Contractor shall analyze potential and actual carrier

network evolution and technology changes. This shall include Contractor investigation, as appropriate, of hybrid networks and technologies. The Contractor shall identify potential impacts of the technological changes on GETS and WPS viability, and the Contractor will continually monitor carrier networks status. As appropriate the Contractor shall evaluate candidate actions to address the impacts and present recommendations to the government.

5.3.2. Service Providers Council (SPC)

SPC Meeting Support: OEC established a Service Providers Council (SPC) under the PTS carrier contracts for the purpose of ensuring Next Generation Network (NGN) Priority Service (PS) priority telecommunications solutions being developed and deployed are interoperable. The SPC consists of AT&T, Verizon, Sprint, the Integration Contractor, T-Mobile, and OEC. OEC requires support for the SPC consisting of engineering assessments and standards support to promote interoperability for NGN priority service feature enhancements. The Contractor, in their role as the IC, shall represent all its service providers under contracts at the SPC. In addition to telecommunications engineering and interoperability standards expertise, the Contractor shall participate in SPC Working Groups (WG). Anticipated WG groups will include, but not be limited to the following: Network to Network Interface (NNI), WPS on VoLTE Performance, future WPS on 5G, GETS on VoIP Performance, NGN Standards, and NGN GETS Wireline Interoperability. Additionally, the Contractor shall support NGN special topics, such as: Authentication, peering and roaming, Apps, user priority levels, handset metrics, use cases, traffic mix, congestion scenarios, Network Function Virtualization (NFV), Software-Defined Networks (SDN), impact of Internet of Things (IoT), vendor equipment settings, TDM and hybrid network performance and schedule for sunsetting, NGN PS Phase 2 for video and data priority, and security. Further engineering expertise is required to research and advise OEC participants of potential issues and to recommend solutions that are standards based such as review, research, and analyze priority services information to provide technical assessments and recommendations for NGN PS enhancements. This support includes identifying and coordinating proprietary and non-proprietary technical and programmatic data from AT&T, Verizon, Sprint, IC (including its subcontractors), T-Mobile, and associated vendors.

5.3.3. Future Services Engineering

The Contractor shall provide engineering to plan for NGN PS for GETS carriers referenced in Paragraph 5.2.1.1 and WPS carriers referenced in Paragraph 5.2.2.1. Contractor shall coordinate sustainment engineering, as appropriate, with AT&T, Sprint, and Verizon through the OEC and the Service Provider Council. The Contractor shall support NS/EP telecommunications requirements by planning for the transition of Legacy PS to NGN PS without experiencing a gap in support and an associated NS/EP telecommunications shortfall. The Contractor shall also support engineering follow-on NGN PS by identifying candidate initiatives that leverage the commercial carrier NGN investments to achieve cost-effective NGN PS solutions.

Contractor's Future Services Engineering shall, include, but not be limited to, the following:

- NGN GETS engineering to analyze carrier network evolution and technology changes to plan follow-on GETS on IP-based networks and, if required, to model planned NGN GETS performance to ensure planned investments will meet the stated objectives.
- NGN MPS (Multi-Media Priority Service) engineering to analyze carrier network evolution and technology changes to plan follow-on NGN WPS (presumed to be 4G LTE and 5G) and, if required, to model planned NGN WPS performance to ensure planned investments will meet the stated objectives.

- Support the Government in developing standards contributions and implementing these standards-based features on GETS and WPS carriers that are on the contract to the Contractor to ensure NGN PS interoperability i.e., network-to-network interface (NNI) to support PS interoperability objectives. The Contractor shall perform actions to implement these features that do not incur implementation costs to the OEC. In those instances in which the Contractor recommends that such implementation that may incur costs, the Contractor shall provide the OEC with a decision brief to initiate a Technology Refreshment contract modification.
- Contribute to NGN PS interfaces and interoperability with FirstNet to meet the objective of interoperability.
- Contribute to NGN PS interfaces to interoperate with other government networks.
- Support optimum PS coverage to meet the objective of affordability that reduces overlap while considering SRAS locations.
- Develop an annual Future Services Plan (FSP) that identifies potential NS/EP priority services investments. For each potential NS/EP investment, the FSP shall include the following:
    - Develops business cases that assesses industry trends and technological advancements, provides an estimated return on investment, identifies the potential for leveraging carrier commercial investments with a leverage factor that estimates the cost savings, judges the lifespan of the potential investment, protects the investment from service provider upgrades, investigates affordable bridging alternative solutions, identifies alternatives to accelerate service to market (Ex. limited operating capability), and utilize a strategy that minimizes risk of chasing technology.
    - Support the government in implementing IP NNIs that will pass NS/EP markers

The Contractor shall include in Carrier Annual Program Reviews a section on future services planning that addresses carrier plans for network and service evolution as they impact evolution to NGN PS.

5.4. Operational Support

The Contractor shall support GETS, SRAS, and WPS performance to meet the stated Program objectives for intra/interagency emergency communications, international interface, interoperability, nationwide coverage, survivability/endurability, and voice-band service. The Contractor shall develop cost-effective methodologies to assess:

- GETS/SRAS and WPS performance to ensure services are operating effectively
- Coverage areas and capacity within those coverage areas are being maintained through network evolution
- User assistance is being provided and user needs are met
- Effective carrier coordination of operations is being achieved through the network operations center
- Timely detection and correction of service problems is being achieved.
- The Contractor shall serve as the central POC for all PS operational measurements and usage data. The Contractor will develop an Operational Plan that documents needed carrier data to assess PS performance, including during crisis and emergencies.

5.4.1. Legacy GETS and WPS Operational Data

The Contractor shall collect, process and archive all legacy GETS and WPS operational measurements and usage data. The Contractor shall develop, operate and maintain applications for data collection and processing and databases for archiving the data. Supported by the Government through the Government's direct contracts with AT&T, Sprint, and Verizon, the Contractor shall reach agreements with AT&T, Sprint, and Verizon for collecting Legacy GETS and WPS operational measurements (OMs) and usage data, and working collaboratively to analyze OMs and usage data, and to identify, track, and resolve service problems. If reaching agreements with ATT, Sprint, or Verizon directly entails costs from any of these carriers, the Contractor shall submit a proposal under Technology Refreshment to the Government that includes these costs.

For legacy GETS call data, the government will arrange for Verizon, AT&T and Sprint to provide GETS call detail records to the Contractor as GFI. The Contractor shall coordinate and compile the GETS call data records and prepare the consolidated data records for government use. The Contractor shall sort call data records by the organizational entities in the PIN/Subscriber database.

5.4.2. NGN PS - NGN GETS (GETS VoIP) and NGN WPS (WPS on VoLTE) Operational Data

The Contractor shall coordinate with the Government to develop a plan to collect, process and archive all NGN PS operational measurements, configuration verification and usage data. The plan shall include, supported by the Government through the Government's direct contracts with AT&T, Sprint, and Verizon, the Contractor reaching agreements with AT&T, Sprint, and Verizon for collecting NG PS operational measurements (OMs) and data, and working collaboratively to analyze OMs and data, and to perform configuration verification. When tasked by the Government, the Contractor shall submit a proposal under Technology Refreshment for executing the plan.

In a separate effort, the Contractor will utilize carrier data to identify, track, and resolve service problems. When tasked by the Government, the Contractor shall submit a proposal under Technology Refreshment for executing the plan.

If the Contractor cannot make arrangements with Verizon, AT&T and Sprint, then the Government shall make arrangements with AT&T, Sprint and Verizon to supply operational data required for the plan. For NGN PS GETS call data, the Government will, if required, arrange for Verizon, AT&T and Sprint to provide GETS call detail records to the Contractor as GFI. The Contractor shall coordinate and compile the GETS call data records and prepare the consolidated data records for government use. The Contractor shall sort call data records by the organizational entities in the PIN/Subscriber database.

The Contractor shall also assess establishing a PS dashboard to monitor service performance from a variety of network feeds. The Contractor shall submit under Optional Technology Refreshment a proposal to implement the dashboard.

5.4.3. GETS Readiness

The Contractor shall seek to maintain user subscription and authentication processes for service readiness at a 100% error free level. To achieve this objective, the Contractor, exclusively, shall perform the following:

- **Create and Manufacture a Secure PIN:** The Contractor shall ensure that each PIN created has a unique 12-digit number.
- **Distribute PINs to Users:** The Contractor shall distribute PINs to users via the POCs to facilitate POC control of the PINs; POCs have the responsibility to distribute the PINs to their users.

- Objective for routine processing - Receive, approve, provision in GETS IXCs, and mail GETS card to POCs for routine requests for activation of GETS subscriptions is ≥90% of routine requests completed within 72 business
- Objective for expedited processing - Receive, approve, provision in GETS IXCs, and mail GETS card to POCs for routine requests for activation of GETS subscriptions is ≥90% of expedited requests completed within 8 business week hours
- **Release PINs to the Networks:** The Contractor shall forward requests to the IXCs with any required PIN data. PIN data provided to the IXCs shall not identify the associated NS/EP Priority Services users or organizations.
- **Update PIN Database:** Upon creation and distribution of PINs, the Contractor shall update the PIN database.
- **Continuously Synchronize PINs and PIN Databases:** The Contractor shall synchronize PINs with the PIN database.
- **Release Partial PIN Databases to POCs:** The Contractor shall release to each POC a partial PIN database consisting of only those PINs issued to that POC.
- **Electronic transfer of PIN data shall be encrypted.**

5.4.4. WPS Readiness

The Contractor shall seek to maintain user subscriptions (approximately 235,000) and authentication process for service readiness at a 100% error free level. To achieve this object, the Contractor, exclusively, shall perform the following:

• Release WPS subscriptions to the Networks. The Contractor shall forward WPS subscriptions to the appropriate WPS service provider for provisioning in the service providers' subscriber database. Only the WPS telephone number and priority level shall be provided to the service provider.

• Update WPS Subscription Database. For each new WPS subscriber, the Contractor shall update Contractor's WPS Subscriber database.

• Quarterly, synchronize service provider WPS subscription information with Contractor's WPS Subscriber Database.

- Objective for routine processing - Receive, approve, and submit to WPS carrier routine requests for activation of WPS subscriptions ≥90% of routine requests completed within 24 business week hours
- Objective for expedited processing – Receive, approve, and submit to WPS carrier expedited requests for activation of WPS subscriptions is ≥90% of expedited requests completed within 8 business week hours.

5.4.5. Security

The Contractor shall maintain PS security by ensuring the following:

- Compliance with GETS and SRAS security classification guides
- Compliance with DHS 4300B, DHS National Security System Handbook
- Carriers maintain PS security through commercial best practices

- Support the new objective of enhanced security by exploring new means for NGN GETS and SRAS security other than PIN use i.e., identity management as part of Future Services Engineering, Paragraph 5.3.3.
- The Contractor shall ensure that only properly authorized persons have access to GETS/WPS data, including GETS and WPS calls records and other performance data.
- The Contractor shall ensure that all GETS card number information is provided the appropriate level of protection against disclosure.
- The contractor shall maintain GWIDS and upgrade its security, as necessary to reduce the probability of a data breach.
- The contractor shall construct and accredit a secure room to administer the PIN database if required.

  Specifically, the Contractor shall perform the following**:**

  - Create a log and log all authentication attempts to access GWIDS
  - Log all changes to user privileges
  - Store the logs in an encrypted table
  - Ensure that the log can only be accessed via an interface to prevent tampering / deletion
  - Develop procedures and algorithms to analyze information in the audit logs
  - Encrypt the connection strings in configuration files to prevent use of the strings in backdoor attacks
  - Conduct SQL injection reviews and penetration tests to identify additional risks to be plugged
  - Encrypt the 12 digit PIN in the unclassified database for transfer and encrypt PIN data when transmitting to POC and carriers
  - Detect re-use of POC accounts by new POCs
  - Encrypt the monthly secure offsite data to ensure it cannot be read if the CDs are stolen in transit
  - Enhance GWIDS to be able to notify users, upon command, in case of a Sensitive Information breach.
  - Expand the log to include the specific data accessed by a GWIDS user
  - Expand the log to include the bulk data exports
  - Develop procedures and algorithms to analyze the above information in the audit logs
  - Conduct additional SQL injection reviews and penetration tests to identify additional risks to be plugged
  - Populate the development and test environments with fictional data versus real GWIDS user data
  - Conduct a privilege escalation review process to minimize the ability of a hacker to obtain “superuser” privileges
  - The Contractor shall support OEC’s effort to obtain and maintain authority to operate (ATO)

5.4.6. Enhanced Operational Support

Contractor shall improve OAM&P application methods and processes, including an enhanced means for measuring service performance. Contractor shall provide:

- A cost-effective service performance monitoring and testing program that ensures Service performance and availability by conducting, and reporting on monthly post-implementation random testing. The post-implementation monitoring and testing shall be conducted using:
  - WPS Remote Service Verification Process (RSVP) system or an equivalent, deployed at multiple sites dispersed nationally.
  - GETS Remote Service Verification Process (RSVP) system or an equivalent, deployed at multiple sites dispersed nationally.
- At the direction of the Government, the Contractor shall coordinate its testing program with AT&T, Verizon, and Sprint, to achieve maximum integration and effectiveness.
- The Contractor shall obtain public call performance so PS performance can be compared to general network performance.
- The performance monitoring and testing processes shall include documenting trouble detection and resolution through the normal OAM&P trouble handling and troubleshooting process.
- Contractor shall maintains WPS phone accounts for WPS RSVP or an equivalent system and OEC testing and report to the government on usage of phones in those accounts.

5.4.7. Enhanced Service Performance Metrics

The Contractor shall:

- Provide and maintain a Performance End-to-End Reporting Service (PEERS) application using “big data analytics” to process, qualify and integrate operational and usage data to produce a measurement of GETS and WPS end-to-end service performance
- Provide and maintain applications and data collection for both GETS/WPS test calls (WPS RSVP) and user calls (PEERS) that assesses PS performance compared to the general public during and after disasters in the focused disaster area.
- Plan the refinement and development of the PEERS approach for assessing end-to-end service performance in a hybrid network where NS/EP calls traverse both circuit and IP-based networks, submit the plan to the Government, and implement the plan when tasked by the Government

The Contractor shall continue to improve OAM&P applications and processes by providing and maintaining web-based reporting of service performance information (PEERS) through a PS Management Dashboard.

5.4.8. Carrier Support

To ensure carrier services meet objectives, and for continuity, the Contractor shall provide operational support for the following carrier requirements to the extent that they are included in carrier agreements. Contractor shall maintain and update, as required by Sustainment Engineering and Technology Refreshment task results, these requirements carried over from the pre-existing carrier subcontracts and re-established under this PWS

- Provisioning Requirements
- OA&M Reporting Requirements.
- Configuration Audits and Reporting Requirements. Contractor shall perform annual configuration audits with each carrier under agreement to provide GETS or WPS. Contractor shall work with carriers to pursue automation of quarterly configuration audits, with corrective measures being taken if errors

are found, to the extent practical. Contractor shall pursue developing a database for archiving network information gathered from the configuration audits and make carrier network information available to the OEC.

- Generic NSVT Test Plans and Reports Requirements. Contractor shall conduct NSVTs annually for each GETS and WPS carrier under subcontract for service, and prepare and submit to the Government a Test Report for each NSVT, with verification data, until such time as NSVTs are integrated with the overall testing program.
- Billing Data Reporting Requirements.
- Call Detail Records Reporting Requirements.
- Annual Carrier Meeting Requirements. Contractor shall conduct Annual Program Reviews with the major carriers under subcontract for GETS and WPS, with virtual meetings preferred. APRs shall review the carrier's past year service performance and future network and services evolution plans.

For GETS configuration data, the Contractor shall continue to provide Configuration Reports.

5.4.9. Testing Service

The Contractor shall develop an integrated and consistent approach to PS operational testing. The Contractor shall serve as the overall tester for PS by developing an affordable testing program.

Operational testing will consist of Legacy GETS and WPS testing, and NG PS testing for WPS on VoLTE and NGN GETS services that are operational at time of contract award.

Developmental, implementation and operational testing would be tasked as part of Technology Refreshment for new and upgraded services being developed and deployed.

As directed by the Government, and supported by the Government through the Government's contracts with AT&T, Sprint and Verizon for the testing program, the Contractor shall conduct testing with AT&T, Sprint, and Verizon for services that are operational at time of contract award.

5.5. Optional Transition Services

5.5.1 Contract Phase In

The Contractor shall participate in a transition period for the Transition Task. During this period the Contractor shall coordinate with the Outgoing Contractor to transition this function to the new Contractor. The Contractor shall coordinate with the OEC and the Outgoing Contractor to determine the approach, major milestones, and schedule for this transition.

To ensure continuous GETS and WPS operations, the Contractor shall pursue placing agreements with the GETS LEC and WPS carriers for commencement, after the current carrier agreements expire.

5.5.2 Contract Phase Out

When tasked by the Government, the Contractor shall prepare a Transition Phase-Out Plan to transition tasks, Government-funded materials including test equipment, and information to an Incoming Contractor or to the Government. The Contractor shall provide requisite support to develop, document, and monitor the execution of the Transition Phase-Out Plan that may be used to transition tasks and materials to a new Contractor, or to the Government. The plan must incorporate an inventory of all services and Government-funded materials developed that are required to fully perform the services provided under this contract. The plan must include a schedule of briefings, including dates and time

and resources allotted, that will be required to fully transition all Government-funded materials developed to the follow-on Contractor, and must provide the names of individuals that will be responsible for fully briefing their follow-on counterparts. The plan must ensure that the follow-on Contractor, and the Government, will be provided sufficient information and be fully briefed prior to the current expiration date of the contract, to provide adequate time for the new Contractor to have its personnel completely familiar with the requirements and in place on the turnover date. The Contractor shall plan for a 90 calendar day transition period. The plan shall provide the contact information for Contractor individuals who will be assigned to the transition team and identify their roles in the transition.

The Contractor shall participate in transition meetings with the Program Manager and project staff, and representatives of the successor Contractor and Government staff. The purpose of these meetings is to review project materials and take preparatory steps to ensure an effective transition of Contractor support. If tasked by the Government a draft transition plan is due to the Government 60 business days prior to the expiration date of the contract to allow for Government review, comment and approval.

5.6. Optional Technology Refreshment

The works described below are all optional.

5.6.1 Technology Refreshment Approach

Under a service-based approach, the Contractor shall pursue the technology refreshment project by specifying service function and performance, rather than a technical solution. The Contractor shall formulate the functional requirements to minimize dictating a specific technical solution and the performance requirements to maximize service operations, performance and performance validation through testing.

The Contractor shall utilize an approved GAO cost methodology to price software related development efforts.

The Contractor shall require the carrier to provide a service specification that describes its compliance to the service and performance specification. The Contractor shall assess the described service for effectiveness and shall deliver the service specification to the Government with the results of the effectiveness assessment as part of the Contractor's proposal for the Technology Refreshment Task.

If authorized to proceed with implementation, the Contractor shall conduct acceptance testing to determine whether the service upgraded with the technology refreshment meets the functional and performance requirements in the subcontract statement of work and the carrier's service specification.

After successful testing, the Contractor shall task the carrier with deploying the technology refreshment and providing the enhanced service.

The Contractor shall require the Service Provider to operate and maintain the subcontracted service, once implemented, throughout the subcontract's Period of Performance. If the Service Provider makes network changes during the subcontract Period of Performance that affect the subcontracted service, Contractor shall require the Service Provider to demonstrate that the network changes do not compromise the service functionality or performance.

For all priority telecommunications service development and deployment initiatives, the Contractor shall be required to follow the Government's prescribed process that follows. The Contractor may propose an alternative cost-savings process that is based on commercial practices if it can be mapped to the process that is hereby described. The Contractor must acquire Government approval for a substitute approach. The Government uses a service acquisition contract strategy based on the requirements

identified in FRS documentation [Ref (a) and (b) below], which includes industry standards. The Contractor may propose using additional industry standards, as well as the standards-like Government Industry Requirements (GIR) documents as the basis for its approach to meet the requirements of the FRS; however, such an approach will be evaluated by the Government and may be used if found to be acceptable. Any vendor development initiated by the Contractor and paid for by the Government shall include Right to Use (RTU) language, where feasible, allowing other carriers, who are also approved by the Government to provide NS/EP Priority Services, to use the resulting development in their own networks at no additional vendor development cost to Government.

The Contractor may propose tailoring the NGN-PS SELC process to better match their own internal SELC processes, Such proposed tailoring will be evaluated by the Government and may be used if found to be acceptable. Regardless, the Contractor shall provide the technical reviews and testing deliverables to the Government as outlined below. Successively developed NGN-PS capabilities may result in multiple design and test reviews. Contractor documentation for design and test reviews, and Government witness testing will be the main deliverables used to verify and validate that requirements are being met. All issues concerning the subject of a review shall be resolved prior to conducting that formal technical review. The Contractor shall support direct on-site attendance at testing events of at least 6 individuals total (Government representatives and support contractors) to serve as Government witnesses. The Contractor may propose, pending Government approval, alternate approaches such as virtual participation in test events, where direct participation by 6 representatives is not possible.

The Contractor shall provide and maintain a Requirements Traceability and Verification Matrix (RTVM) that details how the NGN-PS requirements are being verified and validated at mutually-agreed upon milestones based on specified in references (a) and (b) above and any additional functional requirements agreed upon with the government. This RTVM shall include the Contractor's planned requirements for all functions, capabilities and performance to be implemented for the proposed PS solution. The Contractor shall define interoperability and regression testing requirements drawn from reference (a) that insure the implemented capabilities are compatible with existing priority service capabilities. The Contractor shall incorporate these interoperability and regression testing requirements into the RTVM. This RTVM will be the basis of the design, implementation and testing for the remainder of the Contractor's efforts for the proposed PS. The required verification method for all Reference (b) requirements is Demonstration, as defined in Reference (a).

Using the high-level information provided in its proposal as a basis, the Contractor shall provide a report that thoroughly identifies and describes the risks addressed by proposed priority capabilities and the level of performance improvement and/or risk mitigation expected due to deployment of each capability proposed. The report shall also investigate the potential benefit to NS/EP priority communications of advanced or vendor-customized features which may not specifically be delineated in standards but which still adhere to standards.

Technical Reviews:

The Contractor shall provide a preliminary schedule at the kickoff meeting for conducting technical reviews and update the schedule throughout the duration of this effort in coordination with the government. The Contractor may substitute commercial practices and processes for elements of the DHS SELC process if the Contractor can demonstrate significant savings in terms of cost and time, and/or enhanced performance to the Government. The Contractor shall provide documentation to be approved by the Government that will verify and validate each milestone (i.e., WPS on LTE LC, IOC, and FOC) provided under this tasking. At a minimum, the following technical reviews shall be conducted:

• The Contractor shall conduct a Preliminary Design Review (PDR) for the Government for the LC/IOC/FOC feature development and associated implementation efforts. The PDR allows the Government to evaluate the Contractor's proposed solution, agree on the system requirements, assess whether the Contractor has addressed the functional requirements, review preliminary solution design documentation (objective: 75%), and determine if the solution can be implemented within the cost and schedule constraints.

• The Contractor shall conduct a Critical Design Review (CDR) for the Government for the LC/IOC/FOC feature development and associated implementation efforts. The CDR allows the Government to determine if the design is complete (objective: 95%) and accurate in its documentation specification and can produce the results defined in the baseline requirements. The Contractor shall have resolved all action items from a PDR prior to the CDR. The Government may require changes if the final design solution cannot meet the requirements specified in references (a) and (b) above.

• The Contractor shall conduct a Test Readiness Review (TRR) for the Government prior to each testing event in order to review test plans, assess test objectives, test methods and procedures, scope of tests, determine if required test resources (people, facilities, test articles, test instrumentation) have been properly identified and coordinated to support the test, and otherwise determine the Contractor's readiness for the testing event (e.g., review pertinent documentation, logistics, results from dry runs, etc.). A draft Test Plan is due 60 days before the test or demonstration (unless otherwise negotiated with the Government). The FINAL version of the Test Plan should incorporate all Government comments on the draft Test Plan.

• The Contractor shall conduct a Production Readiness Review (PRR) for the Government after development and testing is complete, and prior to placing the new capabilities in operation.

Testing:

The Contractor shall propose their testing approach and shall establish a schedule for and conduct testing for the proposed PS capabilities as mutually agreed to between the Government and the Contractor. The Contractor shall provide a Handset Validation and Acceptance Test (HVAT) clearly showing that WPS works on mutually-agreed upon user equipment (UEs) commercially available and sold for use on the applicable service provider(s) carrier network(s).

• The Contractor shall provide a Captive Office Test (COT) verifying functional requirements defined in the (RTVM, as well as performance and stress testing of the features to verify they are capable of meeting the Key Performance Parameters (KPPs) in a simulated all-hazards laboratory environment.

• The Contractor shall provide a Networks Services Acceptance Test (NSAT) in a limited production environment to verify correct operation in a live network.

• The Contractor shall conduct testing in accordance with the Government-approved test plans. The Contractor shall allow the Government to witness all testing and have access to test results and all relevant test data. The Government may waive the requirement for Government-witnessed testing for specific testing events based on technical discussions with the Contractor, but this does not relieve the Contractor of the requirement to furnish test results and all relevant test data.

• The Contractor shall define interoperability and regression testing requirements drawn from FRS documentation [Ref (to ensure that the new PS capabilities architecture/solution is backward-compatible with legacy services with no service degradation. The Contractor shall incorporate these interoperability and regression testing requirements into the RTVM, as well as the test plans for COT and NSAT.

• The Contractor shall define what testing may be required during the performance period of the contract for any technology refresh or addition of other pool of non-NS/EP priority users or services implemented by the Contractor in their network which may impact or degrade the proposed PS feature and functionality.

• The Contractor shall define what ongoing Network Service Verification Testing (NSVT) will be implemented during the performance period of the contract to ensure PS features and functionality are configured and operating correctly as the applicable service provider(s) upgrades and deploys new releases of hardware and software in their network.

• The Contractor shall conduct all testing in accordance with the RTVM. The Government will use the RTVM in its acceptance of the Contractor's work.

• The Contractor shall ensure that NGN PS testing is compliant with the Next Generation Network Priority Services Program Test & Evaluation Master Plan.

Deliverables:

The Contractor shall provide the schedule and the documentation for the following required technical reviews:

For the PDR, the Contractor shall deliver the following content and documentation at least 4 weeks before the PDR:

• Preliminary Network Service Architecture (NSA) Document containing:

- Description of the proposed solution and system requirements for NGN-PS features or capabilities, and how they will be integrated to provide both NS/EP communications signaling and traffic higher priority than any other communications, with the exception of network operations .
- Call flow and description of all relationships between subsystems, components, and connections/interfaces/protocols, including those supplied by the applicable service provider's vendors
- Description of equipment configuration for NS/EP traffic and how configuration differentiates NS/EP traffic from public and other high priority users or services.
- Description of any vendor or OEM hardware and software development required for any network element, component, application or feature in Contractor network in order to meet KPPs specified in FRS documentation [Ref (a) and (b) below]. Explanation of why such development is required and how it will be of benefit to NS/EP users in a shared priority services network environment is required. Clarify whether such development is within specific ATIS standards for proposed PS service or functionality, or if ATIS standards would need to be altered to implement and operationalize such development in the applicable service provider(s) network to meet PSKPPs. Identify whether any development may require any United States regulatory or policy changes to meet PS KPPs.
- Preliminary Functional & Performance Analysis from modeling or analysis which verifies performance under anticipated mission environment and benefit of advanced features. Applicable service provider network traffic models during normal busy hours, and alterations in traffic mix for NS/EP-type events should be used, taking into account the operational settings on all hardware and software providing PS features and functionality.
- Preliminary Cybersecurity threat analysis for priority services describing any cyber security vulnerabilities and proposed mitigations for PS, including how malicious traffic will be handled

- Preliminary PS Requirements Gap Analysis that thoroughly identifies and describes the risks addressed by proposed priority capabilities and the level of performance improvement and/or risk mitigation expected due to deployment of each capability proposed. Specific risks and benefits to NS/EP communications as compared to other priority services being offered by the applicable service provider network should be addressed.
- Preliminary High-level Test and Evaluation Plan describing test architecture and equipment, including how function and service performance during congestion load testing will be demonstrated. Applicable service provider network traffic models during normal busy hours, and alterations in traffic mix for NS/EP-type events should be used, taking into account the operational settings on all hardware and software providing PS features and functionality.
- Preliminary Requirements Traceability and Verification Matrix (RTVM)
- Preliminary OAM&P plan and design, including an analysis of requirements and mechanisms to prevent adverse effects on legacy priority services from the addition of new priority services capabilities or contractor network upgrades.
- Updated cost and schedule estimates if there are any changes

For the CDR, the Contractor shall deliver the following documentation, addressing all action items identified during the PDR, at least 4 weeks before the CDR to allow time for review comments and document revisions:

- Final Network Service Architecture Document
- Final High-level Test and Evaluation Plan. Test cases should be listed and be traceable to requirements, either directly or indirectly, and address all defined functions/scenarios/use cases.
- Updated Requirements Traceability and Verification Matrix (RTVM)
- Updated OAM&P plan and design, including an analysis of requirements and mechanisms to prevent adverse effects on legacy priority services from the addition of new priority services capabilities or contractor network upgrades.
- Updated cost and schedule estimates if there are any changes

The Contractor shall hold a TRR prior to each COT or NSAT event. For each TRR, the Contractor shall deliver the following documentation at least 60 days before each TRR to provide sufficient time for review and revision. Test plans should include test objectives specifying which capability is being tested and requirement is being verified; diagram of test and system configuration; description of test equipment required for congestion loading and packet tracing; test location, duration and schedule; test case procedures with expected results and evaluation criteria; and demonstration of cyber security mitigations.

• Final Captive Office Test (COT) plan for performance and stress testing of functional requirements and evaluation of Key Performance Parameters (KPP) under congestion

• Final Network Service Acceptance Test (NSAT) plan for final performance verification of NGN-PS capabilities in a relevant operational environment (e.g. first office, congested event).

For the PRR, the Contractor shall deliver the following documentation at least 60 days before PRR to provide sufficient time for review and revision.

• Final Network Service Architecture Document

• Final Test Results report for each COT or NSAT event.

• Final Requirements Traceability and Verification Matrix (RTVM) with justification for partial or non-compliance or compliance to system requirements or derived requirements; when and what method of verification (e.g., test case, analysis report, modeling, demonstration) verifies the requirement. Compliance to system requirements (derived requirements) should be identified for each vendor used by service provider.

• Final System Engineering and Operations Report (SEOR)

• Describing the final design, how it meets the PS requirements, all COT and NSAT tests and results.

• Show how the testing demonstrated the mitigation of risk by implementing priority service features and show what the performance was during congestion loading. Contractor should provide operational baseline busy hour performance metrics (i.e., KPPs) of commercial users versus NS/EP users measured the tests.

• Final HVAT test results of how all UEs under test performed and interoperated with PS both legacy and new proposed PS enhancements.

• Final OAM&P plan and design, including how the priority service requirements will be maintained when applicable service provider(s) makes equipment software or hardware updates, or changes their network architecture. A network services verification test (NSVT) plan should be included covering regression and verification testing to ensure PS features and functionality are configured and operating correctly as the applicable service provider upgrades and deploys new releases of hardware and software in their network or any technology refresh.

NGN-PS Systems Engineering Life Cycle (SELC) process references

(a) National Security and Emergency Preparedness (NS/EP) Priority Services Functional Requirements Specification (FRS)

(b) National Security and Emergency Preparedness (NS/EP) Priority Services Functional Requirements Specification (FRS), NGN Wireless Priority Access Supplement

5.6.2 Sustain Legacy PS and Deploy NGN PS

The Contractor shall focus on sustaining Legacy priority voice telecommunications services in the nation's TDM-based networks and wireless communications using both GSM/UMTS and CDMA carriers; and, as tasked, to plan, procure, test, and deploy NGN PS.

In performing technology refreshment tasks, the Contractor shall pursue the Government's preferred approach of Service-Based acquisition where appropriate. In other cases, when directed by the Government and in order to derive more benefit from common vendor development, the Contractor shall design and develop vendor solutions with a Right-to-Use buyout.

It is expected that the current wireline and wireless networks will exist in a converged state prior to transitioning to Next Generation Network (NGN) Internet Protocol (IP)-based managed networks. When tasked by the Government, the Contractor shall extend GETS, SRAS, and WPS viability with bridging developments and acquire NGN PS from carriers such as CenturyLink (including legacy tw Telecom), and T-Mobile.

5.6.3 Acquire LTE priority and Full Operation Capability (FOC) on T-Mobile's network

When tasked by the Government, the Contractor shall acquire on T-Mobile's network NS/EP priority service on LTE, specifically WPS on Voice over LTE (VoLTE) Full Operation Capability (FOC).

In acquiring T-Mobile WPS on VoLTE FOC, the Contractor shall consider optional priority for WPS Video and Data on T-Mobile's LTE network. This task shall address T-Mobile's network architecture and topology, and primary functionality for providing the priority service, including QoS mechanisms, protocols, and all network interconnections to support VoLTE, including IXC interoperability, roaming and consideration of WPS video and data on LTE.

The Contractor shall coordinate, to the extent possible with the restrictions of proprietary information, WPS on VoLTE in T-Mobile with the WPS on VoLTE approaches of other carriers through the SPC in order to promote commonality, cost-effectiveness and interoperability.

The OEC is in the process of implementing NS/EP enhancements on T-Mobile's Long Term Evolution (LTE) IP Multimedia Core Network Subsystem (IMS) network to support WPS over VoLTE IOC. T-Mobile's WPS on VoLTE IOC can be characterized as priority access.

The Contractor will acquire, if authorized by the Government through the exercise of this optional task, WPS on VoLTE FOC on T-Mobile's network to provide end-to-end priority for WPS calls on T-Mobile's LTE network. For T-Mobile WPS on VoLTE FOC, as well as all other service provider development and implementation efforts, the Contractor shall follow the NGN-PS Systems Engineering Life Cycle (SELC) Technical Review discussed below. Additionally, The Contractor shall ensure that T-Mobile WPS on VoLTE FOC testing is compliant with the Next Generation Network Priority Services Program Test & Evaluation Master Plan.

5.6.4 TSP Cloud Migration

The primary goal of this acquisition is to migrate the Telecommunications Service Priority Web (TSPWeb) system from the DC1 environment to the Cloud to provide ease of access and enhanced security in support of the TSP Program Office's (TSPPO) its information-sharing objectives as it relates to their National Security and Emergency Preparedness (NS/EP) mission.

The effort is to support current migrations from DC1 to the Cloud as well as providing operations & maintenance (O&M) for TSPWeb. The migration project and O&M will be managed in accordance with the Department of Homeland Security (DHS) security provisions.

Additionally, two-part user authorization will have to be ported from DC1 to the Cloud. And the Contractor shall be responsible for all security in accordance with DHS policy.

5.6.5 GETS, SRAS and WPS

When tasked by the Government, the Contractor shall provide analysis and engineering for technology refreshment with the objectives being:

- To maintain service performance
- To extend service life-cycle
- To add carriers to improve network coverage and availability for NS/EP users
- To increase contractor staffs to support WPS user increases

This effort shall include interoperability planning with AT&T, Sprint, and Verizon though the Service Provider Council.

When tasked by the Government, the Contractor shall support technology refreshment to correct service performance problems and/or service degradation for GETS, SRAS, and WPS by performing the requisite planning, design, engineering, procurement, testing, and implementation/deployment of technology or network upgrades and/or fixes.

For all technology refreshment, the Contractor shall pursue the Government's objective of utilizing a service-based acquisition approach for procuring priority service development, implementation, operations, and performance in an all-hazards environment and through network convergence. Carrier and vendor warranties shall be considered to ensure performance guarantees and to correct identified deficiencies.

5.6.5.1 Right-to-Use Buyout with Warranty

If service-based agreements are not obtainable, at Government direction the Contractor shall pursue the alternative approach of specifying a technical solution and, if needed, conducting NS/EP feature development through Right-to-Use buyout with warranties from vendors and/or carriers.

The Contractor shall coordinate with the appropriate industry vendors and carriers, in coordination with the SPC, to draw upon their expertise in the design and engineering of the technology refreshment and to obtain industry agreement on the solution.

In collaboration with industry, the Contractor shall support development of a consensus Industry Requirements document containing the industry technology refreshment solution.

5.6.5.1.1 Vendor Enhancements

If needed for the Technology Refreshment solution, and as tasked by the Government, the Contractor shall pursue the alternative approach of technology investment though a Right-to-Use (RTU) Buyout, with warranties from vendors and/or carriers.

The Contractor shall coordinate with the Service Provider Council, and other of Contractors' subcontracted service providers, to determine those service providers who would benefit from the RTU Buyout. The Contractor shall, as feasible and appropriate, follow the process for coordinating and conducting RTU Buyouts agreed to by the Service Provider Council.

As appropriate, the Contractor shall perform testing for the vendor enhancements, including arranging with a carrier lab to host Captive Office Testing, and participating and directing Captive Office Testing.

5.6.5.1.2 Carrier Service Acquisition under Right-to-Use with Warranty Approach

The Contractor shall perform service acquisition of the implementation of technology refreshments. The Contractor shall require the carrier to implement the technical solution, utilizing, if applicable, features procured in the Right-to-Use Buyout.

The Contractor shall conduct acceptance testing to determine whether the carrier provisioning of the technology refreshment provides satisfactory service.

After successful testing, the Contractor shall task the carrier with deploying the technology refreshment and providing the enhanced service.

The Contractor shall require the carrier to provide a warranty on the implementation and maintenance of the technology refreshment for the period of performance, including a stipulation that should the service fail as a result of a defect in the implementation or maintenance, the carrier shall correct the defect under the warranty provisions.

5.6.5.2 Adding Carriers to Enhance GETS/SRAS, or WPS Coverage

Upon receiving a contract modification from the government, the Contractor shall add carriers to enhance GETS or WPS coverage by deploying GETS and WPS in alternate carrier networks.

For carriers being added, the Contractor shall pursue the Government objective of utilizing a service-based acquisition approach for procuring priority service development, implementation, operations, and performance in an all-hazards environment and through network convergence

5.6.5.2.1 Service Acquisition Alternative Approach: Right-to-Use Buyout with Warranty

If directed by the government, the Contractor shall pursue service acquisition of additional carriers using the alternate approach of infrastructure investment with warranties in accordance with Section 5.6.2

5.6.5.2 Compatibility with Other PS-Capable Government Communications Networks

When tasked by the Government, the Contractor shall provide technology refreshment to maintain or establish compatibility with other PS capable Government communications networks.

5.6.6 NGN Priority Services

When tasked by the Government, the Contractor shall provide analysis and engineering for technology refreshment to acquire NGN Priority Service for NS/EP users.

5.6.6.1 Technology Refreshment

When tasked by the Government, the Contractor shall provide optional support required for technology refreshment to acquire NGN PS carrier replacements for degrading or decommissioned Legacy GETS, SRAS, and WPS. The Contractor shall provide the requisite planning, procurement, deployment, and testing for NGN PS technology refreshment tasks. The Contractor shall seek to maximize the interoperability of NGN PS with GETS, SRAS and WPS in the service provider's network. The Contractor shall coordinate NGN PS technology refreshment with activities of the Service Provider Council to promote commonality and interoperability of the services from multiple carriers.

For all technology refreshment, the Contractor shall pursue the Government's preferred approach of utilizing a service-based acquisition approach for procuring priority service development, implementation, operations, and performance in an all-hazards environment and through network convergence.

If it is in the Government's best interest and at the direction of the Government, the Contractor may replace the preferred service-based approach, on a case-by-case basis, with a technology approach consisting of: engineering, design, and procurement for development, deployment, and testing.

5.6.6.2 Adding Carriers to Enhance GETS/SRAS, or WPS Coverage

When tasked by the Government, the Contractor shall add services, service providers and/or carriers to enhance GETS, SRAS, or WPS coverage and capacity. When directed by the Government, the Contractor shall procure and deploy PS in carrier and/or service provider networks. For services, carriers and service providers being added, the Contractor shall pursue the Government objective of utilizing performance-based service acquisition (PBSA) strategies. Under PBSA, for contracted services, if a carrier/service provider makes changes to its underlying network architecture for services unrelated NS/EP Priority Services, and then the carrier/service provider shall maintain NS/EP Priority Services functionality within its network without increasing its price for NS/WP Priority Services for the period of performance of the service subcontract. Further, the Contractor shall pursue the Government's objective that priority telecommunications services acquired shall effectively operate within parameters under all circumstances, including crisis or emergency, attack, recovery, and reconstitution, when network congestion or damage renders conventional communications ineffective.

5.6.6.3 Compatibility with Other Government Communications Networks

When tasked by the Government, the Contractor shall provide technology refreshment to maintain and/or establish compatibility with other Government communications networks, including, but not limited to, FirstNet.

5.6.7 Smartphone Applications

When tasked by the Government, Contractor shall develop and provide, as appropriate, smartphone applications, and other applications supporting the Smartphone applications, to enhance existing and follow-on PS: to include, but not limited to:

- Recognition of originated NS/EP calls
- GETS/WPS auto dialer for operating systems and smartphone models beyond those delivered under the previous contract
- GETS/WPS auto dialer with call detail data storage and reporting.
- Other applications as tasked, such as enhancements to the PS Management Dashboard.

Contractor shall provide ongoing application maintenance for the developed Smartphone applications.

5.6.8 NGN PS Wireline (NGN PS Phase 1, Increment 3)

5.6.8.1 NGN PS Wireline Acquisition

The Contractor shall acquire service agreements with carriers to transition Legacy Government Emergency Telecommunications Service (GETS) to the carriers NGN wireline networks. The minimum set of carriers to be included in this initiative are:

TIER 1	**TIER 2**	**TIER 3**
CenturyLink (including legacy carrier: tw Telecom)	Cincinnati Bell	Ben Lomand
	Frontier	East Ascension
	Hawaiian Telecom	GTA Teleguam
	Claro PR	Matanuska
	TDS (Telephone & Data Systems)	Micronesia
		Inteliquent (f. Neutral Tandem)
	Windstream	Pioneer Telephone
		Shentel (Shenandoah Tel)

The wireline carriers identified above have both a wireline “access network” and a “core network”. The focus of this task is the wireline core networks of the wireline carriers. Voice switching functions, whether via IP Multimedia Subsystem (IMS) components, hybrid switching or softswitches, is the most

likely point of congestion, and thus needs National Security and Emergency Preparedness (NS/EP) features. Priority in the wireline access portions of the carriers' networks does not need to be engineered until there is a requirement for priority video and data in the NGN PS. The wireline access will be optional tasking under NGN PS Phase 2, Video and Data.

5.6.8.2 NGN GETS

To sustain GETS in support of the Wireline NGN PS, the following activities will be accomplished:

- **Wireline Core:** To proceed with NGN PS service acquisition, the Contractor shall undertake detailed service engineering and implementation planning with carriers, as follows:
  - Establish detailed network and services baseline
  - Conduct NGN GETS needs analysis and formulation / evaluation of NGN GETS approaches
  - Define NGN GETS Service Specification
  - Complete NGN GETS Implementation Planning
- **Wireline Core Feature Development:** GETS carriers are replacing their Time Division Multiplex (TDM) switches with hybrid (i.e., TDM and Internet Protocol [IP]) switches and IMS components. To sustain GETS, NS/EP features should be developed in the following products that are prevalent in the carriers wireline NGN:
  - Metaswitch
  - BroadSoft Broadworks
  - Ribbon (former Genband C15/G6)
  - IMS Core (Ericsson)

The Contractor shall work with each carrier to determine the optimal selection of features to be defined to maximize cost-effectiveness. Additionally, a goal would be to leverage IMS core functionality already developed for WPS on Voice over Long Term Evolution (VoLTE).

- Wireline Core Initial Operational Capability (IOC) and Full Operational Capability (FOC) Implementation: NGN GETS carriers will need to provision the BroadSoft, Ribbon (former Genband) and Metaswitch components in their networks. NGN GETS carriers will need to provision their IP Network-to-Network Interfaces (NNIs) to ensure NS/EP signaling is carried end-to-end.
- **Wireline Core – IP Enhancements – Planning:** There are a number of efforts that would enhance NGN GETS in wireline networks:
  - Increasing the number of nationwide NGN GETS carriers that can authenticate GETS calls
  - Creating a Resource Priority Header (RPH) authentication token so that NGN GETS carriers know the NGN GETS call request received with an RPH is valid
  - Identifying the IMS Operational Measurements (OMs) needed to analyze, measure and report on GETS performance and readiness
- **Wireline Core – IP Enhancements – Implementation:** Implementing the features from the development effort. This includes increasing the number of NGN GETS carriers to include cable providers; and extending NGN GETS to key transport carriers to ensure that the RPH signaling is transmitted end-to-end.

- **Alternate Carrier Routing (ACR):** When tasked by the Government, the Contractor shall provide recommendations for an NGN ACR replacement.

5.6.9 Acquire LTE priority on US Cellular's network

When tasked by the Government, the Contractor shall acquire on US Cellular's network NS/EP priority service on LTE, specifically Voice over LTE (VoLTE).

The Contractor shall pursue the Government's preferred approach of offering priority service on US Cellular's LTE network in a phased approach. Phasing may be defined as a limited capability (LC) phase, initial operating capability (IOC) phase, and full operating capability (FOC) phase; however, the Contractor is free to propose whatever phases it deems appropriate. The Contractor shall provide priority VoLTE with consideration for optional priority for WPS Video and Data on US Cellular's LTE network. This task shall address US Cellular's network architecture and topology, and primary functionality for proving the priority service, including QoS mechanisms, protocols, and all network interconnections to support VoLTE, including IXC interoperability, roaming and consideration of WPS video and data on LTE.

The Contractor shall coordinate, to the extent possible with the restrictions of proprietary information, WPS on VoLTE in US Cellular's with the WPS on VoLTE approaches of other carriers through the SPC in order to promote commonality, cost-effectiveness and interoperability.

5.6.10 Acquire NGN GETS from Cable Service Providers and Alternative Providers

When tasked by the Government, the Contractor shall acquire NGN GETS network priority services from the following cable service providers, and possible alternative service providers in a phased acquisition:

- COMCAST
- Time Warner
- Cox Communications
- Alternative Service Providers

Phasing may be defined as a limited capability (LC) phase, initial operational capability (IOC) phase, and full operational capability (FOC) phase; however, the Contractor is free to propose whatever phases are deemed appropriate. The Contractor shall acquire and provide priority VoIP with consideration for optional priority for video and data on these cable networks. The task shall address each carrier's network architecture, topology, primary functionality including QoS mechanisms, protocols, and all network interconnections to support VOIP and consideration of priority video and data.

5.6.11 Acquire Video and Data Priority from LECs, Cable Service Providers and Alternative Providers

When tasked by the Government, the Contractor shall acquire video and data network priority services from the following LECs, cable service providers, and possible alternative service providers in a phased acquisition:

- COMCAST
- Time Warner
- Cox Communications
- Alternative Service Providers
- The following LECs:

TIER 1	TIER 2	TIER 3
CenturyLink (including legacy carrier: tw Telecom)	Cincinnati Bell	Ben Lomand
	Frontier	East Ascension
	Hawaiian Telecom	GTA Teleguam
	Claro	Matanuska
	TDS	Micronesia
		Neutral Tandem
	Windstream	Pioneer Telephone
		Shentel
		Consolidated Communications, Mattoon, IL
		Peerless Network

Phasing may be defined as a limited capability (LC) phase, initial operational capability (IOC) phase, and full operational capability (FOC) phase; however, the Contractor is free to propose whatever phases are deemed appropriate. The Contractor shall acquire and provide priority video and data on these cable networks. The task shall address each carrier's network architecture, topology, primary functionality including QoS mechanisms, protocols, and all network interconnections to support priority video and data.

5.6.12 NGN SRAS

When tasked by the Government, the Contractor shall engineer an NGN SRAS solution. The NGN SRAS solution shall include all SRAS TDM capability focusing on maintaining a survivable and robust SRAS solution in a VoIP environment for an NGN SRAS solution.

5.6.13 Vendor Development

When tasked by the Government, the Contractor shall subcontract for support vendor product enhancement for NS/EP priority features through a common development solution with Right-to-Use buyouts.

5.6.14 NGN PS Performance Metrics

When tasked by the Government, the Contractor shall support new approaches for assessing NGN PS performance to include WPS on VoLTE and NGN GETS. When appropriate, methodologies should be US standards-based and align to industry practices. Approaches may include, but not be limited to the following: collecting various OMs, placing an App on user equipment (UE – handsets), using a common vendor for multiple carriers' tool/application to collect performance data, and establishing dashboard(s) to monitor network performance.

5.6.15 Acquire LTE priority on CenturyLink consolidated network including Level 3

When tasked by the government, the Contractor shall acquire NS/EP priority service on CenturyLink's consolidated network including Level 3

The Contractor shall pursue the Government's preferred approach of offering priority service on Level 3's network in a phased approach. Phasing may be defined as a limited capability; however, the Contractor is free to propose whatever phases it deems appropriate. The contractor shall provide NS/EP priority services with consideration for optional priority for Video and Data on Level 3's network. This task shall address Level 3's network architecture and topology, and primary functionality for proving the priority service, including QoS mechanisms, protocols, and all network interconnections to support interoperability.

The Contractor shall coordinate, to the extent possible within restrictions of proprietary information, NS/EP priority services in Level 3's network with the approaches of other carriers through the SPC in order to promote commonality, cost-effectiveness and interoperability.

5.6.16 Sprint and T-Mobile Merger

If Sprint merges with T-Mobile, then the contractor will need to ensure all requirements described in this section (i.e. tasks, deliverables) are provided and transferred under this contract from the DITCO Sprint contract to ensure compliance with FRS. Sprint's T-Mobile merger. If required, the Contractor shall support the migration of the DITCO Sprint contract requirements to this contractor to ensure Sprint PTS is provided and maintained in accordance with the Services Functional Requirements Specification. Specifically, the Contractor shall ensure the requisite Sprint support to accomplish, at a minimum, the following: program management (Including progress reporting, program management reviews, carrier network data acquisition, maintain a quality assurance surveillance plan, provide telecommunications Service Provider Council support, maintain NS/EP priority voice services (Including GETS Interexchange Carrier (IXC) Services and WPS), provide operations, administration, maintenance, and provisioning (OAM&P), conduct performance monitoring, support trouble detection and resolution, perform fraud monitoring and reporting, prepare Trouble/Daily Status Reports, provide call detail records, maintain telecommunication services usage and billing, conduct future services planning, provide GETS Number Translation service and administration, protect the GETS PIN database, support network revisions, conduct network testing, monitor service network performance, and conduct operational testing.

5.6.17 Subscriber Growth

The Contractor shall provide the requisite resources to support greatly increased WPS and WPS VoLTE subscriber growth based on FirstNet user participation and carrier mass activations. The Contractor shall design, enhance automation and increase FTEs to support the growth. Augmented support shall include activations, user support, and service trouble resolution. Specifically, augmentation will require enhancements to the Service Center, Subscription Desk, and Help Desk in order to accommodate massive subscriber growth.

5.7 Service Center

Contractor shall implement, provide, operate and maintain a Service Center, which work shall include:

- Interfacing with service providers
- Interfacing with service user organizations
- Website development and maintenance

- Database development and maintenance.

In support of users, the Contractor shall provide requisite assistance to enhance familiarity, resolve issues, and to surge during disasters and crises to ensure that the cadre of NS/EP users is adequately equipped to benefit from PS.

NOTE: The Service Center provides operational and administrative support to the various priority services programs. The Service Center Concept of Operations identifies the program components and their commonalities, and defines the methodology for consolidated operational and help-desk services under the Service Center. To date, those program components include:

- Government Emergency Telecommunications Service (GETS)
- Wireless Priority Service (WPS)
- Telecommunications Service Priority (TSP)
- Other information about the OEC in general

At the Government's option, when tasked, the Contractor shall expand the scope of the Service Center to include additional priority telecommunications services.

It is anticipated that 95% of this task will support the PS program and 5% will support the Critical Infrastructure Protection's TSP program.

5.7.1 Service Center Support

The Contractor shall provide operational and administrative support to accomplish the mission as outlined under the Service Center CONOPS. These activities may include, but are not limited to the following:

- Follow and expand on the Service Center CONOPS; submit updates to the CONOPS as required
- Maintain and, when tasked, expand the Service Center functionality
- When tasked, the Contractor shall provide additional GETS and WPS operational and administrative support based on the rapidly evolving requirements in order to meet the needs of the targeted NS/EP community and emergency events.

5.7.2 Service Center Support Systems

The Contractor shall:

- Develop and maintain the architecture consolidating technical/information processes of all designated services/programs using web-based technology and a web-based information delivery service
- Continue on-going efforts with the GETS/WPS Administrator to develop and maintain the GETS/WPS Information Delivery Service (G-WIDS)
- Provide maintenance for the POC database applications and support the migration of information and data distribution to the POCs via G-WIDS
- Implement and maintain a Customer Relationship Management Tool (CRMT) for tracking customer information

5.7.3 Customer Service Help Desk

Contractor shall operate and maintain the Customer Service Technical Help Desk. Contractor shall provide Help Desk support to those organizations expressing an interest in subscribing to GETS/WPS and then provide continued technical support to those organizations throughout the establishment and maintenance of those services within their organizations. Help desk shall be maintained with dedicated staff during normal hours with remote backup to consolidated central help desk to provide 24x7x365 assistance. The Contractor will have the capability to surge during disasters to support the help desk with dedicated staff.

The Contractor shall:

- Implement and maintain a remote/backup Call Center to provide Help Desk support
- Provide general customer service support to current and prospective user organizations
- Provide assistance in operations and administration of the services
- Provide assistance to service and agency POCs to ensure regular review/update of GETS cardholders (and WPS where applicable), cancelling accounts for those who have left the organization or no longer qualify for the programs; this includes conducting validations at least annually, to ensure GETS and WPS records are accurate.

5.7.4 Fraud Testing

The Contractor shall perform periodic fraud testing of the GETS process, to ensure compliance with contractual responses to fraud discovery and reporting

5.7.5 Program Information and Support

The Contractor shall:

- Develop and maintain GETS and WPS website content for dissemination of administrative support information and documents
- Update and maintain GETS and WPS program documentation
- Providing assistance in preparing for various programmatic meetings
- Provide processes and procedures necessary to accomplish valued customer service; work includes briefing and meeting preparation and other program support as defined by the Government, e.g., briefing and other preparation assistance for various program oriented meetings, e.g., the GETS/WPS User Council meetings, staff meetings, COP/COR Meetings, and GETS/WPS Team Forums

6.0 QUALITY ASSURANCE SURVEILLANCE PLAN AND PERFORMANCE REQUIREMENTS SUMMARY

The Quality Assurance Surveillance Plan (QASP) and its companion Performance Requirement Summary (PRS), shall be compliant with the Functional Requirements Specifications (FRS). The Performance Requirements Summary (PRS) within the QASP provides performance metrics and quality standards to ensure the required services are achieved by the contractor. The contractor's performance on the quality standards defined in the QASP will be a factor in the determination of the award fee. Anticipated QASP critical factors will focus on availability, readiness, reliability, and performance. The availability objective is defined as always available (0.999% for NS/EP users) 24x7-365 days/year. The

readiness objective is to maintain authentication processes for service readiness at a 100% error free level.

For readiness requirements under the Performance Based Service Acquisition (PBSA), the Acceptable Quality Level (AQL) is established at 100% to ensure the GETS/WPS service parameters and provisioning are error free at all times. The readiness requirements shall be evaluated on the basis of recurring or periodical reporting as well as incident related or exception type reporting. The contractor is expected to propose innovative and cost-effective methodologies for assessing service reliability and performance to achieve call completion objectives for GETS (at 90%) and WPS (at 80%). The contractor is expected to use the performance parameters below for monitoring and measuring during testing and operations for priority voice communications.

NGN PS Key Performance Parameters

Performance Metrics	Performance Objectives	
Metric	**Threshold**	**Objective**
Wireless Call Completion Rate	≥ 0.80	≥ 0.90
Wireline Call Completion Rate	≥ 0.90	≥ 0.95
Wireless Call Quality (Mean Opinion Score)	≥ 3.0 for ≥ 0.90 answered calls	≥ 3.5 for ≥ 0.95 answered calls
Wireline Call Quality (Mean Opinion Score)	≥ 3.5 for ≥ 0.90 answered calls	≥ 4.0 for ≥ 0.95 answered calls
Service Availability	≥ 0.998	≥ 0.999
Expedited User Provisioning	90% of users within 48 hours	95% of users within 48 hours

The Award Fee Plan (Attachment 7) will prescribe the award percentage and award period that is applicable to the PTS tasks. For the Readiness area, no fee will be awarded unless the 100% AQL requirement is met.

The performance objectives will be evaluated every six (6) months through the contract's period of performance. The Award Fee will be based on the Government's assessment of the quality of the contractor's performance for a six (6) month evaluation period. Objective and subjective assessments will be used to evaluate the Contractor's overall performance and corresponding Award Fee during each evaluation period. Determination of the Contactor's performance and Award Fee eligibility will be based on attainment of the subjective performance measures outlined in the PRS (Attachment 6), and further explained in the QASP (Attachment 3)

(End of Section C)

SECTION D – PACKAGING AND MARKING

1.0 MARKING AND DELIVERY

All information submitted to the Government, whether submitted electronically, through the postal system, or in person, shall clearly indicate the Project Title, Contract Number, and the names of the Contracting Officer (CO), Contract Specialist (CS) and Contracting Officer's Representation (COR).

2.0 PAYMENT OF POSTAGE AND FEES

All postage and fees related to submitting information including forms, reports, submittals, etc. to the CO, CS, or the COR shall be paid by the Contractor.

3.0 PACKAGING

Contractor will use best practices for packaging.

(End of Section D)

SECTION E – INSPECTION AND ACCEPTANCE

1.0 INSPECTION OF SERVICES FAR CLAUSE

1.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

The following FAR clauses are available in full text at https://www.acquisition.gov.far/ and are incorporated by reference into this contract:

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.246-4	Inspection of Services – Fixed Price	AUG 1996
52.246-5	Inspection of Services – Cost Reimbursement	APR 1984

Inspection and acceptance of all work and services performed under this contract will be in accordance with the FAR clauses incorporated herein.

2.0 INSPECTION AND ACCEPTANCE CRITERIA

Program manager and/or technical leads will review draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance within the guidelines/requirements of the contract and will inform the Contractor of its acceptability. The Contractor shall ensure the accuracy and completeness of all deliverables in accordance with referenced policy, regulations, laws, and directives. Reports and presentations shall be concise and clearly written. Errors, misleading or unclear statements, incomplete or irrelevant information, and/or excessive rhetoric, repetition, and "padding", or excessive length if a page limit is imposed, shall be considered deficiencies and will be subject to correction by the Contractor at no additional cost to the Government. Unless otherwise indicated, the Government will require 10 workdays to review and comment on deliverables. If the deliverable does not meet the noted criteria, the Government will reject it.

A rejected deliverable will be handled in the following manner:

- After notification that the deliverable did not meet the acceptance criteria the Contractor shall resubmit updated/corrected version 10 workdays after receipt of Government comments.
- Upon the Contractor's re-submission, the Government will reapply the same acceptance criteria.

(End of Section E)

SECTION F – DELIVERABLES OR PERFORMANCE

1.0 PERIOD OF PERFORMANCE

The period of performance for this effort is a one (1) twelve-month base period, with four (4) twelve-month option periods for a total period of performance of five years.

- Base Period: 8/17/2019-8/16/2020
- Option Period 1: 8/17/2020-8/16/2021
- Option Period 2: 8/17/2021-8/16/2022
- Option Period 3: 8/17/2022-8/16/2023
- Option Period 4: 8/17/2023-8/16/2024

2.0 PLACE OF PERFORMANCE

Work performed under this contract will primarily be performed at Contractor facilities, with allowances for frequent local travel between the Contractor's office facilities and DHS facilities in the Washington, DC metropolitan area is expected.

3.0 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 9:00 AM and 5:30 PM Eastern Time (ET), Monday through Friday (except Federal Holidays). However, there may be occasions when contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under the PTS PWS.

4.0 DELIVERABLES

Deliverables shall be in accordance with requirements contained in Section C and listed in Attachment 2.

- No proprietary standards shall be referenced or used in the generation of any deliverables.
- Regarding all deliverables, if the delivery date falls on a Saturday or Holiday, which is on a day other than a Monday, the deliverable will be considered to have been received by the Government on the preceding workday. If the delivery date falls on a Sunday or a Monday holiday, the deliverable will be considered to be received on the following workday.
- The contractor shall submit each deliverable as one file, unless file size or other conditions warrant establishing multiple files and submit the table of contents in the same file as the main body of the deliverable. All deliverables must have a document control number and revision number.
- In the event the contractor anticipates difficulty in complying with any delivery schedule, the contractor shall immediately notify the Contracting Officer in writing, giving pertinent details, including the date by which it expects to make delivery; provided, however, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.

5.0 FAR CLAUSES

The following clauses are incorporated by reference:

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.211-8	Time of Delivery	JUN 1997
52.242-15	Stop Work Order (Alternate I – APR 1984)	AUG 1989
52.242-17	Government Delay of Work	APR 1984
52.247-34	F.O.B. Destination	NOV 1991

(End of Section F)

SECTION G – CONTRACT ADMINISTRATION DATA

1.0 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The Contracting Officer has designated the COR to assist in monitoring the work under this contract. The COR is responsible for the administration of the contract and technical liaison with the Contractor. The COR IS NOT authorized to change the scope of work or specifications as stated in the contract, to make any commitments or otherwise obligate the Government or authorize any changes which affect the contract cost/price, delivery schedule, period of performance or other terms or conditions.

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds. The technical administration of this contract shall not be construed to authorize the revision of the terms and conditions of this contract. Any such revision will be authorized in writing by the Contracting Officer.

Contract Officer (CO): Toya Reynolds (Toya.Reynolds@hq.dhs.gov) 202-447-5666

Contract Specialist (CS): Matthew Wetzel (Matthew.Wetzel@hq.dhs.gov) 202-447-0944

Contracting Officer's Representative (COR): TBD After Award

2.0 CONTRACTING OFFICER'S (CO) AUTHORITY

A warranted Contracting Officer is the only person authorized to issue modifications to the contract, approve changes in any of the requirements, or obligate funds. Notwithstanding any clause/provision contained elsewhere in this contract, the authority to modify the contract remains solely with the Contracting Officer. If the Contractor makes any contract changes at the direction of any person other than the Contracting Officer, the change will be considered to have been made without authority and no adjustment will be made in the contract to cover any increases in charges that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the contract in accordance with its terms and conditions.

3.0 SUBMISSION OF INVOICES

All invoices shall be submitted in PDF via email to:

NPPDInvoice.Consolidation@ice.dhs.gov
All invoices must be addressed as follows:
Burlington Finance Office
P.O. Box 1279
Williston, VT 05495-1249
Attn: NPPD-CS&C

The Contractor shall provide invoices for all Accountable Personal Property within 30 days of acquisition to the Property Administrator (PA) and COR.

All invoices shall contain the CLIN and Accounting Classifications, contract number, purchase order number, Supplier's name, Supplier's phone number, manufacturer, manufacturer part number, manufacturer model number, serial number, quantities, item descriptions, and unit cost

The purchase order number shall be on all invoices, packages, bills of lading, correspondence, and any other documents pertaining to the contract

Separate invoices are required for each purchase order

All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and ENERGY Star standards. Scope qualifies for DHS CATEX A5 and B3. These CATEXs should be noted in the project file and also stated in future ITAR submission in support of this contract.

The contractor shall invoice once a month (1st of the month) for the Firm Fixed Price CLINs. The contractor shall invoice monthly based on actual costs for the cost portion of the Cost Plus Award Fee CLINs.

The contractor shall include the following on its invoices:

(a) Name and address of contractor.

(b) Invoice date and number;

(c) Contract number, contract line item number and, the order number;

(d) Description, quantity, unit of measure, unit price, and extended cost/price of supplies delivered or services performed;

(e) Shipment number and date of shipment, including the bill of lading number and weight of shipment if shipped on Government bills of lading.

(f) Terms of any discount for prompt payment offered;

(g) Name and address of official to whom payment is to be sent;

(h) Name, title, phone number of person to notify in the event of a defective invoice; and

(i) Taxpayer Identification Number (TIN) on the invoice.

(j) Electronic Funds Transfer (EFT) banking information.

(A) The contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.

(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer—Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer—Other Than Central Contractor Registration), or applicable agency procedures.

(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

Any other information or documentation required by the contract.

Cost reimbursement vouchers shall be submitted in accordance with FAR 52.216-7, Allowable Cost and Payment, and must specify at a minimum, the following information for the billing period:

1. The total cost/price billed for the current billing period;

2. A breakdown by cost element for the current billing period, the current fiscal year, and the contract to date;

3. The cumulative cost/price billed for the current fiscal year; and the cumulative cost/price billed for the contract to date.

4. Current and cumulative costs must be shown at the task level

5. A completion voucher must be submitted for each invoice in accordance with FAR 52.216-7.

6. The Contractor shall map each cost invoiced to the corresponding task/subtask in the SOO and PWS paragraph with the corresponding CLIN in each invoice.

7. The Contractor shall provide supporting documentation (receipts) for travel being invoiced during the billing period.

8. The cover or summary page of the invoice shall include a statement similar to the following: "As an authorized corporate official of [name of Contractor], I certify to the above invoiced amount is true and accurate for the period identified herein."

Invoices without the above information will be returned for resubmission. Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

- Contracting Officer (CO): Toya Reynolds (Toya.Reynolds@hq.dhs.gov)
- Contract Specialist (CS): Matthew Wetzel (Matthew.Wetzel@hq.dhs.gov)
- Contracting Officer's Representative (COR): TBD After Award

4.0 GOVERNMENT-FURNISHED PROPERTY (GFP)/ GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide Government-Furnished Property (GFP) if the mission requires, the Contractor requests, and the COR concurs. Upon completion of this contract, the Contractor shall submit, to the Program Office, a complete inventory of all GFP remaining in their possession. The Program Office will provide disposition instructions on all property furnished and/or purchased under this contract.

GFI (software, manuals, drawings, test data, etc.) will be provided at Contractor's request or when the mission requires. The list shall include description (title, data, and author), quantities and license numbers. Upon completion of this contract, the Contractor shall submit, to the Program Office, a complete inventory and all GFI remaining in their possession under the contract. The Program Office will provide disposition instructions on all property furnished or purchased under this contract. For access to GFI during the solicitation process, please see Reading Room Instructions (Attachment 8)

See complete list of GFP and GFI for this requirement in Attachment 4.

4.1 Definitions:

• Accountable Personal Property - An asset that meets one or more of the following criteria: (1) expected useful life is two years or longer and an asset value and/or acquisition cost of $5,000 or more; (2) that is classified as sensitive; (3) for which accountability or property control records are maintained; (4) Capitalized personal property, (5) Leased property that meets accountability standards, or (6) otherwise warrants tracking in the property system of record. Current accountable personal property information may be obtained through the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov.
• Capitalized Personal Property - Non-expendable personal property with an acquisition cost over an established threshold and a normal life expectancy of two years or more. Current Capitalization Threshold information may be obtained through the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov.
• Contract Property - Contract property refers to both Contractor-Acquired Property (CAP) and GFP, in the possession of contractors.
• Contractor Acquired Property (CAP) - Property acquired, fabricated, or otherwise provided by the contractor for performing a contract and to which the Government has title.
• Government Furnished Property (GFP) - Property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. NOTE: GFP may also be referred to as Government Furnished Equipment (GFE), the two terms are interchangeable.
• Leased Property - Property that is not owned by DHS, but that is leased by the Government under terms as stipulated in the lease agreement (this excludes the leasing of property by contractors in the performance of a contract).
• Sensitive Personal Property - All items, regardless of value, that require special control and accountability due to unusual rates of loss, theft, or misuse; national security or export control considerations. Such property includes but is not limited to, weapons, ammunition, explosives, information technology equipment with memory capability, cameras, and communications equipment. Current sensitive personal property information may be obtained through the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov.

4.2 Property Accountability:
• When contractors are furnished with GFP, DHS barcodes will not be removed. In all GFP cases, the Government retains title to the property
• It is the contractor’s responsibility to use contract property as it was authorized, and for the purpose intended. In the event the contractor uses contract property for other purposes without written authorization from the CO, the contractor may be liable for rental, without credit, of such items for each month or part of a month in which such unauthorized use occurs

• Contractor is directly responsible and accountable for all contract property in its possession in accordance with the requirements of the particular contract; this also includes any contract property in the possession or control of a subcontractor
• Physical inventory: In addition to requirements provided under the contract's government property clause:
• The Contractor shall, minimum annually, perform, record, and disclose physical inventory results of CAP and GFP to the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov, PA and/or COR
•Annual inventory results will be completed, certified and submitted by close of business 31 May each year to the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov, PA and/or COR
• The Contractor shall, upon request, perform, record, and disclose physical inventory results of CAP and GFP to the CS&C APO Office cs&cassetmanagementteam@hq.dhs.gov., PA and/or COR
• As requested inventory results will be completed, certified and submitted, in the timeframe defined at the time of request, to the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov., PA and/or COR

4.3 Property Disposal:
• All documentation and goods are the property of the United States Government and, if applicable, the contractor shall return or destroy appropriately upon request. The contractor shall comply with applicable government rules and regulations for disposal of government property. Further, the contractor shall provide necessary information to the PA, COR and the CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov. For all excess property prior to taking any action. Excess personal property" means any personal property under the control of a Federal agency that the agency head determines is not required for its needs or for the discharge of its responsibilities.
• Lost, Stolen, Damaged or Destroyed (LDD) property:
• Unless otherwise provided in the contract, the contractor is liable for LDD of contract property, except for reasonable wear and tear in accordance with the contract's government property clause.
• Any occurrence of LDD must be investigated and fully documented by the PA and/or COR, who will promptly notify the CO. The contractor will submit a report of any incident of LDD contract property to the PA in accordance with the contract's government property clause and as detailed below, as soon as it becomes known
• When GFP or CAP property is LDD, the Contractor must report within 24 hours of discovery of the event to the COR who will initiate a Report of Survey. This document will be obtained from CS&C APO Office at cs&cassetmanagementteam@hq.dhs.gov.
• A Report of Survey will be prepared, regardless whether or not preliminary research of a LDD event indicates positive evidence of negligence, misconduct, or unauthorized use and the responsible individual refuses to admit pecuniary liability.
• The Contractor must forward this document with all supporting documentation to the PA or COR within 5 business days of the LDD event for review.
• The PA and/or COR must submit the completed package to cs&cassetmanagementteam@hq.dhs.gov.within 5 business days of receipt from the Contractor.
• Contractor, PA and/or COR must supply all requested information and any subsequent requests for information.

(End of Section G)

SECTION H – SPECIAL CONTRACT REQUIREMENTS

1.0 SECURITY REQUIREMENTS

All Contractor personnel assigned to this task shall be U.S. citizens and all proposed personnel shall have a minimum of SECRET clearance. Select Key Personnel will be required to have TOP SECRET/ SENSITIVE COMPARTMENTED INFORMATION for select tasks (as notated below is Section 16.3).

Security shall be in accordance with the Contract Security Classification specification DD Form 254.

1.1 GENERAL

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at a DHS or other Government Facility, it shall abide by the requirements set by the agency.

Access to national security information is required for tasks in this SOW during the period of performance for this contract; CS&C will coordinate with the Office of Selective Acquisition security manager (OSASM) in issuing the DD 254 prior to the commencement of work and any special-handling requirements of information that will be provided to personnel or subcontractors.

The DHS Office of the Chief Security Officer (OCSO) has primary security cognizance of all work performed during the performance of this contract unless otherwise directed by the government.

The contractor shall be required to hold and maintain a Secret Facility Clearance Level (FCL).

- Identification/Building Pass

  The Contractor shall coordinate with the COR to assure that any Contractor employee requiring access to the DHS offices has a Contractor identification/building pass before the employee enters on duty under the contract. Personnel designated by the COR shall complete appropriate forms specified by the DHS Office of Security for security clearance requirements. The Contractor shall see that all passes are returned to the Government as employees are dismissed, terminated or when the need for the employee to have access to DHS offices ceases.
- Security Instructions

  The procedures outlined below shall be followed for the DHS Security Office to process background investigations and suitability determinations, as required, in a timely and efficient manner.

1.2 Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

1.3 Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity

analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the DHS Security Office. Prospective Contractor employees shall submit the following completed forms to the DHS Security Office. The Standard Form 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Security Office no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, sub-contractor employee, or vendor:

- Standard Form 85P's must be given to Public Trust Positions
- FD Form 258, 85P's must be given to Public Trust Positions (2 copies)
- DHS Form 11000-6's must be given to Public Trust Positions no less than thirty (30) days before the start date of the contract
- DHS Form 11000-9's must be given to Public Trust Positions no less than thirty (30) days before the start date of the contract

Only complete packages will be accepted by the DHS Security Office. Specific instructions on submission of packages will be provided upon award of the contract.

DHS shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization shall follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office. Contract employees assigned to the contract not needing access to sensitive DHS information or recurring access to DHS' facilities shall not be subject to security suitability screening.

Contract employees awaiting an EOD decision may begin work on the contract provided they do not access sensitive Government information. Limited access to Government buildings is allowable prior to the EOD decision if the contractor is escorted by a Government employee. This limited access is to allow contractors to attend briefings, non-recurring meetings and begin transition work.

1.4 The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to who it was issued and the last known location and disposition of the pass or card.

1.5 When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive

data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

1.5.a.1 Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the Government do not relieve a Contractor from performing under the terms of the contract.

1.5.a.2 Your POC at the Security Office is: Tarvin Greene, (703) 705-6398

All services provided will be in accordance with DHS Management Directive 4300.l as implemented by DHS 4300A and/or 4300B Policies and Handbooks.

- Access to DHS IT Systems is governed by DHS 4300A
- Sensitive Systems Policy, and DHS 4300B, DHS National Security System Handbook.

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information**.**

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.l Safeguarding Sensitive but Unclassified (For Official Use Only) Information, describes how Contractors must handle sensitive but unclassified information. DHS MD 4300.l Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering Contractors specifically for all contracts that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the Contractor except as specified in the contract.

1.6 Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized COR, and other Government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of Government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

2.0 BACKGROUND INVESTIGATIONS

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual shall perform on the contract. All of the Contractors' employees will be required to pass DHS suitability requirements. PIV cards will be required for all contractor staff accessing DHS network or facility, but not all on this procurement. The Program Office will provide the contractors with the proper security paperwork for obtaining the PIV cards and will ensure that all PIV cards are returned at the end of the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted.

All background investigations shall be processed through the Security Office. Prospective Contractor employees shall submit the following completed forms to the Security Office through the COR no less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form 85P, "Questionnaire for Public Trust Positions"
- FD Form 258, "Fingerprint Card" (2 copies)
- Conditional Access to Sensitive But Unclassified Information
- Non-Disclosure Agreement
- Disclosure and Authorization Pertaining to Consumer Reports

2.1 Pursuant to the Fair Credit Reporting Act

Required forms shall be provided by DHS at the time of award of the contract. Only complete packages shall be accepted by the Security Office. Specific instructions on submission of packages shall be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to or development of any DHS IT system. DHS shall consider only U.S. Citizens and LPRs for employment on this contract. DHS shall not approve LPRs for employment on this contract in any position that requires the LPR to access or assist in the development, operation, management or maintenance of DHS IT systems. By signing this contract, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

The security requirements for this contract include:

A. Personnel security
B. Information technology security
C. Facility security

Standard U.S. Government security clauses will apply. All contractor employees performing work under this contract must be U.S. Citizens.

3.0 EMPLOYEE IDENTIFICATION

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as a Contractor when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

4.0 INFORMATION TECHNOLOGY ACQUISITION REVIEW (ITAR)

4.1 Interconnection Security Agreements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, or interconnect service agreements.

4.2 Security Requirements for Unclassified Information Technology Resources

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services by which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security

Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the Contractor during the contract, and certify that all non-public DHS information has been purged from any Contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the Contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 11.0, January 14, 2015) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

4.3 Contractor Employee Access

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, “Policies and Procedures of Safeguarding and Control of SSI,” as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as “For Official Use Only,” which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person’s privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated “sensitive” or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) “Information Technology Resources” include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer’s Technical Representative (COTR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COTR in writing as necessary for performance of the work under this contract. Any attemPS by contractor personnel to gain access to any information

technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COTR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

4.4 Federal Desktop Core Configuration (FDCC)

All hardware and software shall be Federal Desktop Core Configuration (FDCC) compatible.

4.5 DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

(1) All developed solutions and requirements shall be compliant with the HLS EA.

(2) All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

(3) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

(4) Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

(5) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

4.6 EnergyStar

All hardware procured directly or in support of this action must meet applicable and appropriate EPEAT and ENERGY Star standards

5.0 INFORMATION SECURITY

DHS 4300A Policy 1.5.1.a This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

DHS 4300A Policy 3.3.a All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.

DHS 4300A Policy 3.3.b Contractor information system services and operations shall adhere to all applicable DHS information security policies.

DHS 4300A Policy 3.3.d SOWs and contracts shall include a provision stating that, when the contract ends, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system(s) that have been used to process DHS information.

DHS 4300A Policy 3.3.j All SOW, contract vehicles, and other acquisition-related documents shall include privacy requirements and establish privacy roles, responsibilities, and access requirements for contractors and service providers.

DHS 4300A Policy 4.1.1.a Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.

DHS 4300A Policy 4.1.1.c Components shall ensure any Federal employee granted access to any DHS system has a favorably adjudicated Tier 2 Investigation (formerly Moderate Risk Background Investigation [MBI]) as defined in DHS Instruction 121-01-007, Personnel Suitability and Security

Program, Chapter 2, Federal Employee/Applicant Suitability Requirements. In cases where non-DHS Federal employees have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 2, paragraph G). Active duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military Justice (UCMJ) shall be exempt from this requirement.

DHS 4300A Policy 4.1.2.a Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.

DHS 4300A Policy 4.1.2.b Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.

DHS 4300A Policy 4.1.5.b DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) accessing DHS systems shall receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness training within 24 hours of being granted a user account. If a user fails to meet this training requirement, user access shall be suspended.

DHS 4300A Policy 4.1.5.c DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) shall receive initial specialized training and thereafter annual refresher training specific to their security responsibilities.

DHS 4300A Policy 4.1.5.f User accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training, unless a waiver is granted by the Component's Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM).

DHS 4300A Policy 4.1.5.l The annual security awareness training shall include incident response training to information system users consistent with assigned roles and responsibilities. (Initial training shall be completed within twenty-four (24) hours of assuming an incident response role or responsibility. Out of cycle refresher training shall be conducted as required due to information system changes)

DHS 4300A Policy 4.2.1.d Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

DHS 4300A Policy 4.2.1.e These requirements shall extend to DHS assets located at non-DHS facilities or non-DHS assets and equipment that host DHS data.

DHS 4300A Policy 4.3.1.c DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (such as USB drives) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.

DHS 4300A Policy 4.3.1.e DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)

DHS 4300A Policy 4.8.3.a Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.

6.0 PRIVACY PROVISIONS

6.1 SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Definitions. As used in this clause—

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as

amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status

(4) Ethnic or religious affiliation

(5) Sexual orientation

(6) Criminal History

(7) Medical Information

(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be “sensitive” depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) Authorities. The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) Handling of Sensitive Information. Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how Contractors must handle sensitive but unclassified information. DHS uses the term “FOR OFFICIAL USE ONLY” to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program

responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

(4) The Contractor's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the COR or other Government personnel associated with the administration of the contract, as needed.

(e) Authority to Operate. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

• Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

• Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST

Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

• Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) Security Review. The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Continuous Monitoring. All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its

location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and infrastructure.

(5) Revocation of ATO. In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) Federal Reporting Requirements. Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the Contracting Officer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractor has failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime contractor location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

(g) Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The Contractor shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

(h) Additional PII and/or SPII Notification Requirements.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to Government analysis of the incident and the terms of its instructions to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

(i) Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the Contractor or resided in the Contractor IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) Certification of Sanitization of Government and Government-Activity-Related Files and Information. As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)

6.2 **INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015**)

(a) Applicability. This clause applies to the Contractor, its subcontractors, and Contractor employees (hereafter referred to collectively as "Contractor"). The Contractor shall insert the substance of this clause in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, Contractor and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new Contractor employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The Contractor shall maintain signed copies of the DHS Rules of Behavior for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, the Contractor shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the COR will provide notification when a review is required.

(c) Privacy Training Requirements. All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

7.0 SECTION 508

7.1 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

7.2 Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

7.3 Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

7.4 Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some, but not all, of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of

products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

8.0 ADVERTISMENTS, PUBLICIZING AWARDS AND NEWS RELEASES

Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity/ news release or commercial advertising without first obtaining explicit written consent to do so from the Contracting Officer. This restriction does not apply to marketing materials developed for presentation to potential government customers of this contract.

The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

9.0 OBSERVANCE OF LEGAL HOLIDAYS AND ADMINISTRATIVE LEAVE

The Department of Homeland Security observes the following days as holidays:

New Year's Day
Martin Luther King's Birthday
Washington's Birthday
Memorial Day
Independence Day
Labor Day
Columbus Day
Veterans Day
Thanksgiving Day
Christmas Day

Any other designated by Federal Law, Executive Order, or Presidential Proclamation.

When any holiday specified above falls on a Saturday, the preceding Friday shall be observed. When any such holiday falls on a Sunday, the following Monday shall be observed. Observances of such days by Government personnel shall not be cause for additional period of performance or entitlement to compensation except as set forth in the contract. If the contractor's personnel work on a holiday, no form of holiday or other premium compensation will be reimbursed either as a direct or indirect cost, unless authorized pursuant to an overtime clause elsewhere in the contract.

(DHS may close a DHS facility for all or a portion of business day as a result of granting administrative leave to non-essential DHS employees (e.g., unanticipated holiday); inclement weather; failure of Congress to appropriate operational funds; Or any another reason

In such cases, contractor personnel not classified as essential, i.e., not performing critical round-the-clock services or tasks, who are not already on duty at the facility, shall not report to the facility. Such contractor personnel already present shall be dismissed and shall leave the facility.

10.0 NON-PERSONAL SERVICES

The Government and the Contractor understand and agree that the services delivered by the Contractor to the Government are non-personal services. The parties also recognize and agree that no employer-employee or master-servant relationship exists or will exist between the Government and the Contractor. The Contractor and the Contractor's employees are not employees of the Federal Government and are not eligible for entitlement and benefits given federal employees.

Contractor personnel under this contract shall not (i) be placed in a position where there is an appearance that they are employed by a Federal Officer, or are under the supervision, direction, or evaluation of a Federal Officer, or (ii) be placed in a position of command, supervision, administration, or control over Government personnel.

11.0 IDENTIFICATION OF CONTRACTOR PERSONNEL

The Contractor shall ensure that its employees will identify themselves as employees of their respective company while working on DHS/OPO contracts. For example, contractor personnel shall introduce themselves in person and in voice-mail, and sign attendance logs as employees of their respective companies, and not as DHS employees. The Contractor shall ensure that their personnel use the following format signature on all official e-mails generated by DHS computers:

Name

Position or Professional Title

Company Name

Supporting the (INSERT PROGRAM OFFICE NAME; I.E., DHS/CISA/ECD)

12.0 PRINTING RESTRICTIONS

All printing funded by this contract must be done in conformance with Joint Committee on Printing regulations as prescribed in Title 44, United States Code, and Section 308 of Public Law 101-163, and all applicable Government Printing Office and Department of Homeland Security regulations.

13.0 PRODUCT IMPROVEMENT/TECHNOLOGY ENHANCEMENT

(a) At any time during the performance of this contract, the Contractor may submit, or DHS may request a Product Improvement/Technology Enhancement proposal for review. The Contractor is encouraged to discuss product improvement/ technology enhancement ideas with the Integrated Product Team prior to preparing and submitting a formal proposal. These proposals should suggest methods for performing more economically and/or methods for incorporating emerging technology. Changes may be proposed to save money, to improve performance or reliability, to save energy or

space, to satisfy increased data processing requirements, to incorporate technological advances in software, or for other technical or business reasons that the Contractor believes may be advantageous to DHS. Discontinuance of equipment is subject to negotiations and to DHS written approval prior to the introduction of a substitute product.

(b) The Government is not liable for proposal preparation costs or any delay in acting upon any proposal. The Contractor has the right to withdraw, in whole or in part, any proposal not accepted by DHS within the period specified in the proposal. The decision of the Contracting Officer as to the acceptance or rejection of a proposed change is final and not subject to dispute. Proposals must be valid for at least 30 days.

(c) Any proposed change may be approved, in whole or in part, and the change incorporated into a contract modification signed by both parties. The contract modification will include an equitable adjustment for the resultant costs or savings and modify any other affected provision of the contract. Until the effective date of the modification, the Contractor shall perform in accordance with the existing contract.

(d) As a minimum, the following information should be submitted by the Contractor with each proposal. The extent and detail provided should be proportionate to the complexity and/or value of the proposed change.

(1) A description of the difference between the existing contract requirement and the proposed change, and the comparative advantages and disadvantages of each;

(2) A discussion of the functions of the modeling tool, facilities, services and supplies for the purpose of achieving the essential functions at the lowest life cycle cost and consistent with required performance, reliability, quality, and safety;

(3) Itemized requirements of the contract, which must be changed if the proposal is adopted, and the proposed revision to the contract for each such change;

(4) An estimate of the changes in performance and cost/price, if any that will result from adoption of the proposal;

(5) An evaluation of the effects the proposed change would have on collateral costs to the Government, such as costs of related items, and costs of maintenance and operation;

(6) A statement of the time by which the change order adopting the proposal must be issued so as to obtain the maximum benefits of the changes during the remainder of the contract;

(7) A statement of the effect on the contract completion date or delivery schedule;

(e) A reasonable method for sharing in the proposed savings, if any, if the proposed change would result in a reduction in the overall life cycle costs.

14.0 POST AWARD EVALUATION OF CONTRACTOR PERFORMANCE

14.1 Electronic Access to Contractor Performance Evaluations

FAR 42.15 require agencies to prepare annual and final evaluations of contractor performance. The U.S. Department of Homeland Security utilizes the National Institutes of the Health (NIH) Contractor

Performance System (CPS) to record and maintain past performance information. Contractors that have Internet capability may access evaluations through a secure Web site for review and comment by completing the registration form that can be obtained at the following URL: http://www.cpars.gov

The registration process requires the contractor to identify an individual that will serve as a primary contact and who will be authorized access to the evaluation for review and comment. In addition, the contractor will be required to identify a secondary contact who will be responsible for notifying the cognizant contracting official in the event the primary contact is unavailable to process the evaluation within the required 30-day time period. Once the contractor is registered and a performance evaluation has been prepared and is ready for comment, the CPS will send an email to the contractor representative notifying that individual that a performance evaluation is electronically available for review and comment.

15.0 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the CO, CS and COR no later than ten (10) business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the CO, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan.

16.0 CONTRACTOR PERSONNEL

16.1 Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOO/PWS. The contractor shall maintain the personnel, organization, and administrative control necessary to ensure that the work delivered meets the government's specifications and requirements. The work history of each contractor employee must contain experience directly related to work him/she is required to perform under this contract.

The Government reserves the right, during the life of this contract, to request work histories on any contractor employee for the purposes of verifying compliance with the above requirements; additionally, the government reserves the right to review resumes of contractor personnel (only key personnel) proposed to be assigned to this contract.

16.2 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer Representative (COR) prior to an employee's absence. Otherwise, the Contractor shall provide a fully qualified replacement.

16.3 Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor shall notify the COR and Contracting Officer no less than 15 days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed

substitutes shall possess qualifications equal to or superior to those of the Key person being replaced. The Contractor shall not replace Key Contractor personnel without acknowledgment from the Contracting Officer. The following positions are designated as Key for this requirement:

- Program Manager (Secret)
- Sustainment Engineering Lead (Secret and TS/SCI)
- WPS Lead (Secret)
- OAM&P Lead (Secret and TS/SCI)

Contractor Key personnel shall not be assigned by the Contractor to more than one key position for this requirement. The Government may designate additional Contractor personnel as key during the life of any resulting contract by a bilateral modification.

Key Personnel minimum qualifications are as follows:

Program Manager (Secret Clearance)

The following education and experience are required for the contract Program Manager:

• A Bachelor's Degree in Management, Engineering or Communications. Certifications related to project management, such as Project Management Professional (PMP) certification are required and other related certifications are highly desirable. Background must reflect that the experience and knowledge is current with respect to IP networks.

• A minimum of 8 years of experience in telecommunications, preferably IP-based, acquisition, negotiation, planning, design, implementation, and operations, with a nationwide public switched telecommunications (PSTN) network carrier (preferred).

• Program management experience providing senior systems engineering and technical support in telecommunications, acquisition, planning, design, implementation, and operations of priority telecommunications services and applications on commercial voice networks.

• Experience with current GETS/SRAS and WPS requirements (as appropriate).

• The ability to prepare complex and professional documentation concerning voice network technology trends, new services, carrier network upgrade timelines and their impacts or enhancements to existing or future GETS, SRAS, and WPS services.

• Experience in managing and writing highly technical documentations to acquire services and features similar to PTS.

• Experience in reviewing and commenting on the technical feasibility, pricing, and schedule of vendor and carrier proposals and experience in organizing and presenting technical briefings to senior management to support strategic PTS program decisions.

• Extensive knowledge of major wireless and wireline networks, services, and pricing, and experience with public switched telephone network interworking and interfaces, for both packet (preferred) and circuit switched architectures, and a working knowledge of VoIP communications.

• Experience in user applications, design, deployment, and operations of wireline emergency telephone systems and mobile public safety and priority communications networks.

• Understanding of Telecom Network Operations and billing processes.

• Specific experience with National Security and Emergency Preparedness (NS/EP) type communications involving network damage, network congestion, network security and network management.

• Specific experience in gathering and documenting user requirements and translating into contract requirements.

Sustainment Engineering Lead (Secret and TS/SCI Clearance)

The following education and experience are required for the Lead Sustainment Engineer:

• A Bachelor of Science Degree in Engineering. Additional certifications related to current network management, operation, and/or security.

• A minimum of 5 years of technologically –relevant experience in telecommunications acquisition, planning, design, implementation, and operations, preferably with a major carrier or top-tier equipment vendor.

• Experience with current GETS/SRAS and WPS requirements (as appropriate).

• Experience with implementation and operations of Local Exchange Carrier (LEC) and Interexchange Carrier voice networks, particular emphasis given to packet switched network architectures, and experience specifically in dealing with congestion and network reporting processes. Legacy circuit switched network experience also a plus.

• Experience with analyzing and reporting of network problems affecting flow and delivery of priority emergency traffic.

• Specific experience with GETS/SRAS and WPS requirements.

• Experience working with Tier 2 and Tier 3 wireline and wireless service providers and the unique challenges they face to provide special features to the USG that are interoperable with Tier 1 providers in order to create end to end priority service.

• Experience supporting National Security (NS)/Emergency Preparedness (EP) requirements.

• Experience with vendor and carrier lab testing, carrier testing, and other field-testing of new features and services is very important.

• Ability to write, define, and manage oversight of network metrics and Key Performance Indicators (KPI).

• Experience with technology trends and long-term strategic initiatives of carriers and vendors, including Voice over IP (VoIP), and network virtualization.

WPS Lead (Secret Clearance)

The following education and experience are required for the WPS Lead:

• A Bachelor of Science Degree in Engineering. Certifications related to network engineering are highly desirable.

• A minimum of 5 years of technologically–relevant experience in wireless telecommunications acquisition, planning, design, testing, implementation, and operations, preferably with a nationwide domestic mobile operator or top-tier equipment vendor.

• Experience with current GETS/SRAS and WPS requirements (as appropriate).

• Experience with implementation and operations of wireless networks, particular emphasis on LTE networks, legacy 3G networks (CDMA, UMTS) also a plus.

• Experience specifically in dealing with wireless network vulnerabilities to include loading and congestion for signaling access and transport services, and experience with traffic reporting and other network measurements.

• Experience with commercially deployed Radio Access Network (RAN) technologies and experience with subscriber profiles/capacity baseline metrics, and functional understanding of network elements – for LTE this includes the elements of the RAN, Evolved Packet Core (EPC) and IP Multimedia Subsystem (IMS).

• Understanding of traffic and signaling call flows, particular emphasis on IP-based networks, and understanding of and experience with Network metrics and Key Performance Indicators (KPI).

• Experience in user applications, design, deployment, operations of mobile public safety and priority communications networks and experience with Radio Frequency (RF) and network capacity planning modeling software.

OAM&P Lead (Secret and TS/SCI Clearance)

The following education and experience are required for the OAM&P Lead:

• A Bachelor of Science Degree in Engineering or Operations Research Degree.

• A minimum of 5 years of technologically-relevant experience in wireline and wireless telecommunications acquisition, planning, design, implementation, and operations, preferably with a major telecommunications carrier.

• Experience with current GETS/SRAS and WPS requirements (as appropriate).

• Experience with implementation and operation of currently deployed networks, where emergencies, exercises, readiness and contingencies are the primary service along with the experience to define and evaluate effective metrics. The ability to design and analyze operational measurements from such networks and emergency capabilities is essential, including extensive experience with communications transport functions provided by the US interexchange carriers.

• Experience with support to emergency communications should include a strong background with network control and management centers providing user help functions and trouble ticket type resolution.

• Experience with testing of new features as part of pre and post implementation.

• Broad experience dealing with subscriber profiles, subscriber applications, and subscriber trends is very important and highly desirable.

• Experience in managing and writing technical documentation supporting service performance and problem resolution.

• Specific experience in writing and enforcing Service Level Agreements (SLAs) with associated metrics and performance criteria.

• Specific experience in gathering and documenting user requirements and translating into contract requirements.

All Contractor personnel assigned to this task shall be U.S. citizens and all proposed personnel shall have a minimum of SECRET clearance. Select Key Personnel will be required to have TOP SECRET/ SENSITIVE COMPARTMENTED INFORMATION for select tasks (in accordance with Section 16.3).

16.4 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

16.5 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

16.6 Terminations/Resignations

The Contractor shall notify the Site Security Officer (SSO), COR and Contracting Officer of all terminations/resignations of contractor personnel assigned to this contract five (5) working days before the last day of employment. In the event this notification is not possible, the SSO and COR should be notified immediately. The Contractor shall return to the SSO all DHS-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the SSO and COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

17.0 DISCLOSURE OF "OFFICIAL USE ONLY" INFORMATION SAFEGUARDS

Any Government information made available or to which access is provided, and which is marked or should be marked "Official Use Only", shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Disclosure to anyone other than an officer or employees of the Contractor or Subcontractor at any tier shall require prior written approval of the Contracting Officer. Requests to make such disclosure shall be addressed to the Contracting Officer.

Each officer or employee of the Contractor or Subcontractor at any tier to whom "Official Use Only" information may be made available or disclosed shall be notified in writing by the Contractor that "Official Use Only" information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such "Official Use Only" information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to ten years or both.

18.0 TRAINING

The Government will not allow costs, nor reimburse costs associated with the Contractor training employees in an effort to attain and/or maintain minimum personnel qualification requirements of this contract**.**

19.0 CHANGES DUE TO FUNDING SHORTFALLS

(a) The Contracting Officer may at any time, by written order, and without notice to the sureties, if any, make changes within the general scope of this contract in schedule due to funding shortfalls or compliance with restrictions on funding.

(b) If any such change causes an increase or decrease in the estimated cost of, or the time required for, performance of any part of the work under this contract, whether or not changed by the order, or otherwise affects any other terms and conditions of this contract, the Contracting Officer shall make an equitable adjustment in the

(1) estimated cost, delivery or completion schedule, or both;

(2) amount of any award fee; and

(3) other affected terms and shall modify the contract accordingly.

(c) The Contractor must assert its right to an adjustment under this clause within 30 days from the date of receipt of the written order. However, if the Contracting Officer decides that the facts justify it, the Contracting Officer may receive and act upon a proposal submitted before final payment of the contract.

(d) Failure to agree to any adjustment shall be a dispute under the Disputes clause. However, nothing in this clause shall excuse the Contractor from proceeding with the contract as changed.

(e) Notwithstanding the terms and conditions of paragraphs (a) and (b) above, the estimated cost of this contract and, if this contract is incrementally funded, the funds allotted for the performance of this contract, shall not be increased or considered to be increased except by specific written modification of the contract indicating the new contract estimated cost and, if this contract is incrementally funded, the new amount allotted to the contract. Until this modification is made, the Contractor shall not be obligated to continue performance or incur costs beyond the point established in the Limitation of Cost or Limitation of Funds clause of this contract.

20.0 CFR 252.234-7002 Earned Value Management System

(a)Definitions. As used in this clause –

Acceptable earned value management system means an earned value management system that generally complies with system criteria in paragraph (b) of this clause.

Earned value management system means an earned value management system that complies with the earned value management system guidelines in the ANSI/EIA-748.

Significant deficiency means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b)System criteria. In the performance of this contract, the Contractor shall use -

(1) An Earned Value Management System (EVMS) that complies with the EVMS guidelines in the American National Standards Institute/Electronic Industries Alliance Standard 748, Earned Value Management Systems (ANSI/EIA-748); and

(2) Management procedures that provide for generation of timely, reliable, and verifiable information for the Contract Performance Report (CPR) and the Integrated Master Schedule (IMS) required by the CPR and IMS data items of this contract.

(c) If this contract has a value of $50 million or more, the Contractor shall use an EVMS that has been determined to be acceptable by the Cognizant Federal Agency (CFA). If, at the time of award, the Contractor's EVMS has not been determined by the CFA to be in compliance with the EVMS guidelines as stated in paragraph (b)(1) of this clause, the Contractor shall apply its current system to the contract and shall take necessary actions to meet the milestones in the Contractor's EVMS plan.

(d) If this contract has a value of less than $50 million, the Government will not make a formal determination that the Contractor's EVMS complies with the EVMS guidelines in ANSI/EIA-748 with respect to the contract. The use of the Contractor's EVMS for this contract does not imply a Government determination of the Contractor's compliance with the EVMS guidelines in ANSI/EIA-748 for application to future contracts. The Government will allow the use of a Contractor's EVMS that has been formally reviewed and determined by the CFA to be in compliance with the EVMS guidelines in ANSI/EIA-748.

(e) The Contractor shall submit notification of any proposed substantive changes to the EVMS procedures and the impact of those changes to the CFA. If this contract has a value of $50 million or more, unless a waiver is granted by the CFA, any EVMS changes proposed by the Contractor require

approval of the CFA prior to implementation. The CFA will advise the Contractor of the acceptability of such changes as soon as practicable (generally within 30 calendar days) after receipt of the Contractor's notice of proposed changes. If the CFA waives the advance approval requirements, the Contractor shall disclose EVMS changes to the CFA at least 14 calendar days prior to the effective date of implementation.

(f) The Government will schedule integrated baseline reviews as early as practicable, and the review process will be conducted not later than 180 calendar days after -

(1) Contract award;

(2) The exercise of significant contract options; and

(3) The incorporation of major modifications.

During such reviews, the Government and the Contractor will jointly assess the Contractor's baseline to be used for performance measurement to ensure complete coverage of the statement of work, logical scheduling of the work activities, adequate resourcing, and identification of inherent risks.

(g) The Contractor shall provide access to all pertinent records and data requested by the Contracting Officer or duly authorized representative as necessary to permit Government surveillance to ensure that the EVMS complies, and continues to comply, with the performance criteria referenced in paragraph (b) of this clause.

(h) When indicated by contract performance, the Contractor shall submit a request for approval to initiate an over-target baseline or over-target schedule to the Contracting Officer. The request shall include a top-level projection of cost and/or schedule growth, a determination of whether or not performance variances will be retained, and a schedule of implementation for the rebaselining. The Government will acknowledge receipt of the request in a timely manner (generally within 30 calendar days).

(i)Significant deficiencies.

(1) The Contracting Officer will provide an initial determination to the Contractor, in writing, on any significant deficiencies. The initial determination will describe the deficiency in sufficient detail to allow the Contractor to understand the deficiency.

(2) The Contractor shall respond within 30 days to a written initial determination from the Contracting Officer that identifies significant deficiencies in the Contractor's EVMS. If the Contractor disagrees with the initial determination, the Contractor shall state, in writing, its rationale for disagreeing.

(3) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer's final determination concerning -

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action;

(iii) System noncompliance, when the Contractor's existing EVMS fails to comply with the earned value management system guidelines in the ANSI/EIA-748; and

(iv) System disapproval, if initial EVMS validation is not successfully completed within the timeframe approved by the Contracting Officer, or if the Contracting Officer determines that the Contractor's earned value management system contains one or more significant deficiencies in high-risk guidelines in ANSI/EIA-748 standards (guidelines 1, 3, 6, 7, 8, 9, 10, 12, 16, 21, 23, 26, 27, 28, 30, or 32). When the Contracting Officer determines that the existing earned value management system contains one or more significant deficiencies in one or more of the remaining 16 guidelines in ANSI/EIA-748 standards, the contracting officer will use discretion to disapprove the system based on input received from functional specialists and the auditor.

(4) If the Contractor receives the Contracting Officer's final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the significant deficiencies.

(j)Withholding payments. If the Contracting Officer makes a final determination to disapprove the Contractor's EVMS, and the contract includes the clause at 252.242-7005, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(k) With the exception of paragraphs (i) and (j) of this clause, the Contractor shall require its subcontractors to comply with EVMS requirements as follows:

(1) For subcontracts valued at $50 million or more, the following subcontractors shall comply with the requirements of this clause:

< TBD If Applicable>

(2) For subcontracts valued at less than $50 million, the following subcontractors shall comply with the requirements of this clause, excluding the requirements of paragraph (c) of this clause:

< TBD If Applicable>

(End of Section H)

SECTION I – CONTRACT CLAUSES

1.0 FAR PROVISIONS / CLAUSES INCORPORATED BY REFERENCE

FAR 52.252-1 Solicitation Provisions Incorporated By Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): https://www.acquisition.gov/browse/index/far

FAR 52.252-2 Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): https://www.acquisition.gov/browse/index/far

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.202-1	Definitions	NOV 2013
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions on Subcontractor Sales to the Government	SEP 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price or Fee Adjustment for Illegal or Improper Activity	MAY 2014
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2015
52.203-14	Display of Hotline Poster(s)	OCT 2015
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.203-17	Contractor Employee Whistleblower Rights and Requirement to Inform Employee Of Whistleblower Rights	APR 2014
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	JAN 2017
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-12	Unique Entity Identifier Maintenance	OCT 2016

52.204-13	System for Award Management Maintenance	OCT 2016
52.204-14	Service Contract Reporting Requirements	OCT 2016
52.204-18	Commercial and Government Entity Code Maintenance	JUL 2016
52.204-19	Incorporation by Reference of Representations and Certifications	DEC 2014
52.204-22	Alternative Line Item Proposal	JAN 2017
52.204-23	Prohibition of Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	JUL 2018
52.209-2	Prohibition on Contracting with Inverted Domestic Corporations - Representation	NOV 2015
52.209-6	Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment	OCT 2015
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations	NOV 2015
52.210-1	Market Research	APR 2011
52.215-2	Audit and Records - Negotiation	OCT 2010
52.215-8	Order of Precedence – Uniform Contract Format	OCT 1997
52.215-10	Price Reduction for Defective Certified Cost or Pricing Data	AUG 2011
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data—Modifications	AUG 2011
52.215-12	Subcontractor Certified Cost or Pricing Data	OCT 2010
52.215-13	Subcontractor Certified Cost or Pricing Data—Modifications	OCT 2010
52.215-14	Integrity of Unit Prices (Alternate I – OCT 1997)	OCT 2010
52.215-15	Pension Adjustments and Asset Reversions	OCT 2010
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other Than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data—Modifications (Alternate III OCT 1997)	OCT 2010
52.215-22	Limitations on Pass-Through Charges – Identification of Subcontract Effort	OCT 2009
52.215-23	Limitations on Pass-Through Charges	OCT 2009
52.216-7	Allowable Cost and Payment	JUN 2013
52.216-10	Incentive Fee	JUN 2011
52.217-2	Cancellation Under Multi-Year Contracts	OCT 1997
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.219-9	Small Business Subcontracting Plan	JAN 2017
52.219-28	Post-Award Small Business Program Rerepresentation	JUL 2013
52.222-2	Payment for Overtime Premiums	JUL 1990
52.222-3	Convict Labor	JUN 2003
52.222-21	Prohibition of Segregated Facilities	APR 2015

52.222-26	Equal Opportunity	SEP 2016
52.222-37	Employment Reports on Veterans	FEB 2016
52.222-50	Combating Trafficking in Persons	MAR 2015
52.222-54	Employment Eligibility Verification	OCT 2015
52.222-62	Paid Sick Leave Under Executive Order 13706	JAN 2017
52.223-5	Pollution Prevention & Right-To-Know Information	MAY 2011
52.223-6	Drug-Free Workplace	MAY 2001
52.223-10	Waste Reduction Program	MAY 2011
52.223-15	Energy Efficiency In Energy-Consuming Products.	DEC 2007
52.223-16	Acquisition of EPEAT®-Registered Personal Computer Products	OCT 2015
52.223-18	Encouraging Contractor Policies to Ban Text Messaging While Driving	AUG 2011
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.224-3	Privacy Training	JAN 2017
52.225-13	Restrictions on Certain Foreign Purchases	JUN 2008
52.227-1	Authorization and Consent (Alternate II – APR 1984)	DEC 2007
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	DEC 2007
52.227-14	Rights in Data—General (Alternate IV – DEC 2007)	MAY 2014
52.227-16	Additional Data Requirements	JUN 1987
52.227-17	Rights in Data – Special Works	DEC 2007
52.227-18	Rights In Data – Existing Works	DEC 2007
52.227-21	Technical Data Declaration, Revision, and Withholding of Payment—Major Systems	MAY 2014
52.227-22	Major System—Minimum Rights	JUN 1987
52.227-23	Rights to Proposal Data (Technical)	JUN 1987
52.228-7	Insurance—Liability to Third Persons	MAR 1996
52.229-3	Federal, State, and Local Taxes	FEB 2013
52.230-2	Cost Accounting Standards	OCT 2015
52.230-6	Administration of Cost Accounting Standards	JUN 2010
52.232.1	Payments	APR 1984
52.232.6	Payment under Communication Service Contracts with Common Carriers	APR 1984
52.232.8	Discounts for Prompt Payments	FEB 2002
52.232.9	Limitation on Withholdings of Payments	APR 1984
52.232-11	Extras	APR 1984
52.232-17	Interest	MAY 2014
52.232-20	Limitation of Cost	APR 1984
52.232-22	Limitation of Funds	APR 1984
52.232-23	Assignment of Claims	MAY 2014
52.232-25	Prompt Payment (Alternate I – FEB 2002)	JUL 2013
52.232-33	Payment by Electronic Funds Transfer—System for Award Management	JUL 2013
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013

52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013
52.233-1	Disputes	MAY 2014
52.233-3	Protest after Award (Alternate I – JUN 1985)	AUG 1996
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	APR 1984
52.237-3	Continuity of Services	JAN 1991
52.237-11	Accepting and Dispensing of $1 Coin	SEP 2008
52.239-1	Privacy or Security Safeguards	AUG 1996
52.242-1	Notice of Intent to Disallow Costs	APR 1984
52.242-3	Penalties for Unallowable Costs	May 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-5	Payments to Small Business Subcontractors	JAN 2017
52.242-13	Bankruptcy	JUL 1995
52.243-1	Changes—Fixed Price (Alternate I – APR 1984)	AUG 1987
52.243-2	Changes—Cost Reimbursement (Alternate I – APR 1984)	AUG 1987
52.243-7	Notification of Changes	JAN 2017
52.244-2	Subcontracts (Alternate I – JUN 2007)	OCT 2010
52.244-5	Competition in Subcontracting	DEC 1996
52.244-6	Subcontracts for Commercial Items	JUL 2018
52.245-1	Government Property	JAN 2017
52.245-9	Use and Charges	APR 2012
52.246-20	Warranty of Services	MAY 2001
52.246-25	Limitation of Liability—Services	FEB 1997
52.247-63	Preference for U.S.-Flag Air Carriers	JUN 2003
52.247-67	Submission of Transportation Documents for Audit	FEB 2006
52.248-1	Value Engineering (Alternate II – FEB 2000)	OCT 2010
52.249-2	Termination for Convenience of the Government (Fixed-Price)	APR 2012
52.249-6	Termination (Cost-Reimbursement)	MAY 2004
52.249-8	Default (Fixed-Price Supply and Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.253-1	Computer Generated Forms	JAN 1991

The following FAR Clauses are incorporate using full text:

52.204-1 Approval of Contract (DEC 1989)

This contract is subject to the written approval of Contracting Officer and shall not be binding until so approved.

(End of clause)

52.204-21 Basic Safeguarding of Covered Contractor Information Systems (JUN 2016)

(a) Definitions. As used in this clause--

“Covered contractor information system” means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

“Federal contract information” means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

“Information” means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

“Safeguarding” means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

52.217-9 Option to Extend the Term of the Contract (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days prior to exercise the option; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five (5) years.

(End of Clause)

52.222-35 Equal Opportunity for Veterans (OCT 2015)

(a) Definitions. As used in this clause--

“Active duty wartime or campaign badge veteran,” “Armed Forces service medal veteran,” “disabled veteran,” “protected veteran,” “qualified disabled veteran,’ and “recently separated veteran” have the meanings given at FAR 22.1301.

(b) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60-300.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified protected veterans, and requires affirmative action by the Contractor to employ and advance in employment qualified protected veterans.

(c) Subcontracts. The Contractor shall insert the terms of this clause in subcontracts of $150,000 or more unless exempted by rules, regulations, or orders of the Secretary of Labor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate of identify properly the parties and their undertakings.

[Class Deviation- 2017-O0008, Office of Federal contract Compliance Programs Waiver of Certain Clause Requirements in Contracts for Hurricane Harvey Relief Efforts. This clause deviation is effective on Sept 01, 2017, and remains in effect until incorporated into the FAR, or otherwise rescinded.

(d) Notwithstanding the provisions of this section, the Contractor will not be obligated to develop the written affirmative action program required under the regulations implementing the Vietnam Era Veterans’ Readjustment Assistance Act (VEVRAA).

(End of Clause)

52.222-36 Equal Opportunity for Workers with Disabilities (JUL 2014)

(a) Equal opportunity clause. The Contractor shall abide by the requirements of the equal opportunity clause at 41 CFR 60.741.5(a), as of March 24, 2014. This clause prohibits discrimination against qualified individuals on the basis of disability, and requires affirmative action by the Contractor to employ and advance in employment qualified individuals with disabilities.

(b) Subcontracts. The Contractor shall include the terms of this clause in every subcontract or purchase order in excess of $15,000 unless exempted by rules, regulations, or orders of the Secretary, so that such provisions will be binding upon each subcontractor or vendor. The Contractor shall act as specified by the Director, Office of Federal Contract Compliance Programs of the U.S. Department of Labor, to enforce the terms, including action for noncompliance. Such necessary changes in language may be made as shall be appropriate to identify properly the parties and their undertakings.

[Class Deviation- 2017-O0008, Office of Federal contract Compliance Programs Waiver of Certain Clause Requirements in Contracts for Hurricane Harvey Relief Efforts. This clause deviation is effective on Sept 01, 2017, and remains in effect until incorporated into the FAR, or otherwise rescinded.

(c) Notwithstanding the provisions of this section, the Contractor will not be obligated to develop the written affirmative action program required under the regulations implementing section 503 of the Rehabilitation Act of 1973, as amended.

(End of Clause)

52.232-32 Performance Based Payments (APR 2012)

(a) Amount of payments and limitations on payments. Subject to such other limitations and conditions as are specified in this contract and this clause, the amount of payments and limitations on payments shall be specified in the contract's description of the basis for payment.

(b) Contractor request for performance-based payment. The Contractor may submit requests for payment of performance-based payments not more frequently than monthly, in a form and manner acceptable to the Contracting Officer. Unless otherwise authorized by the Contracting Officer, all performance-based payments in any period for which payment is being requested shall be included in a single request, appropriately itemized and totaled. The Contractor's request shall contain the information and certification detailed in paragraphs (l) and (m) of this clause.

(c) Approval and payment of requests.

(1) The Contractor shall not be entitled to payment of a request for performance-based payment prior to successful accomplishment of the event or performance criterion for which payment is requested. The Contracting Officer shall determine whether the event or performance criterion for which payment is requested has been successfully accomplished in accordance with the terms of the contract. The Contracting Officer may, at any time, require the Contractor to substantiate the successful performance of any event or performance criterion which has been or is represented as being payable.

(2) A payment under this performance-based payment clause is a contract financing payment under the Prompt Payment clause of this contract and not subject to the interest penalty provisions of the Prompt Payment Act. The designated payment office will pay approved requests on the 30th day after receipt of the request for performance-based payment by the designated payment office. However, the designated payment office is not required to provide payment if the Contracting Officer requires substantiation as provided in paragraph (c)(1) of this clause, or inquires into the status of an event or performance criterion, or into any of the conditions listed in paragraph (e) of this clause, or into the Contractor certification. The payment period will not begin until the Contracting Officer approves the request.

(3) The approval by the Contracting Officer of a request for performance-based payment does not constitute an acceptance by the Government and does not excuse the Contractor from performance of obligations under this contract.

(d) Liquidation of performance-based payments.

(1) Performance-based finance amounts paid prior to payment for delivery of an item shall be liquidated by deducting a percentage or a designated dollar amount from the delivery payment. If the

performance-based finance payments are on a delivery item basis, the liquidation amount for each such line item shall be the percent of that delivery item price that was previously paid under performance-based finance payments or the designated dollar amount. If the performance-based finance payments are on a whole contract basis, liquidation shall be by either predesignated liquidation amounts or a liquidation percentage.

(2) If at any time the amount of payments under this contract exceeds any limitation in this contract, the Contractor shall repay to the Government the excess. Unless otherwise determined by the Contracting Officer, such excess shall be credited as a reduction in the unliquidated performance-based payment balance(s), after adjustment of invoice payments and balances for any retroactive price adjustments.

(e) Reduction or suspension of performance-based payments. The Contracting Officer may reduce or suspend performance-based payments, liquidate performance-based payments by deduction from any payment under the contract, or take a combination of these actions after finding upon substantial evidence any of the following conditions:

(1) The Contractor failed to comply with any material requirement of this contract (which includes paragraphs(h) and (i) of this clause).

(2) Performance of this contract is endangered by the Contractor's-

(i) Failure to make progress; or

(ii) Unsatisfactory financial condition.

(3) The Contractor is delinquent in payment of any subcontractor or supplier under this contract in the ordinary course of business.

(f) Title.

(1) Title to the property described in this paragraph (f) shall vest in the Government. Vestiture shall be immediately upon the date of the first performance-based payment under this contract, for property acquired or produced before that date. Otherwise, vestiture shall occur when the property is or should have been allocable or properly chargeable to this contract.

(2) "Property," as used in this clause, includes all of the following described items acquired or produced by the Contractor that are or should be allocable or properly chargeable to this contract under sound and generally accepted accounting principles and practices:

(i) Parts, materials, inventories, and work in process;

(ii) Special tooling and special test equipment to which the Government is to acquire title;

(iii) Nondurable (i.e.,noncapital) tools, jigs, dies, fixtures, molds, patterns, taps, gauges, test equipment and other similar manufacturing aids, title to which would not be obtained as special tooling under paragraph (f)(2)(ii) of this clause; and

(iv) Drawings and technical data, to the extent the Contractor or subcontractors are required to deliver them to the Government by other clauses of this contract.

(3) Although title to property is in the Government under this clause, other applicable clauses of this contract (e.g.,the termination clauses) shall determine the handling and disposition of the property.

(4) The Contractor may sell any scrap resulting from production under this contract, without requesting the Contracting Officer's approval, provided that any significant reduction in the value of the property to which the Government has title under this clause is reported in writing to the Contracting Officer.

(5) In order to acquire for its own use or dispose of property to which title is vested in the Government under this clause, the Contractor shall obtain the Contracting Officer's advance approval of the action and the terms. If approved, the basis for payment (the events or performance criteria) to which the property is related shall be deemed to be not in compliance with the terms of the contract and not payable (if the property is part of or needed for performance), and the Contractor shall refund the related performance-based payments in accordance with paragraph (d) of this clause.

(6) When the Contractor completes all of the obligations under this contract, including liquidation of all performance-based payments, title shall vest in the Contractor for all property (or the proceeds thereof) not-

(i) Delivered to, and accepted by, the Government under this contract; or

(ii) Incorporated in supplies delivered to, and accepted by, the Government under this contract and to which title is vested in the Government under this clause.

(7) The terms of this contract concerning liability for Government-furnished property shall not apply to property to which the Government acquired title solely under this clause.

(g) Risk of loss. Before delivery to and acceptance by the Government, the Contractor shall bear the risk of loss for property, the title to which vests in the Government under this clause, except to the extent the Government expressly assumes the risk. If any property is lost (see 45.101), the basis of payment (the events or performance criteria) to which the property is related shall be deemed to be not in compliance with the terms of the contract and not payable (if the property is part of or needed for performance), and the Contractor shall refund the related performance-based payments in accordance with paragraph (d) of this clause.

(h) Records and controls. The Contractor shall maintain records and controls adequate for administration of this clause. The Contractor shall have no entitlement to performance-based payments during any time the Contractor's records or controls are determined by the Contracting Officer to be inadequate for administration of this clause.

(i) Reports and Government access. The Contractor shall promptly furnish reports, certificates, financial statements, and other pertinent information requested by the Contracting Officer for the administration of this clause and to determine that an event or other criterion prompting a financing payment has been successfully accomplished. The Contractor shall give the Government reasonable opportunity to examine and verify the Contractor's records and to examine and verify the Contractor's performance of this contract for administration of this clause.

(j) Special terms regarding default. If this contract is terminated under the Default clause, (1)the Contractor shall, on demand, repay to the Government the amount of unliquidated performance-based payments, and (2)title shall vest in the Contractor, on full liquidation of all performance-based payments, for all property for which the Government elects not to require delivery under the Default clause of this contract. The Government shall be liable for no payment except as provided by the Default clause.

(k) Reservation of rights.
(1) No payment or vesting of title under this clause shall-
(i) Excuse the Contractor from performance of obligations under this contract; or

(ii) Constitute a waiver of any of the rights or remedies of the parties under the contract.

(2) The Government's rights and remedies under this clause-

(i) Shall not be exclusive, but rather shall be in addition to any other rights and remedies provided by law or this contract; and

(ii) Shall not be affected by delayed, partial, or omitted exercise of any right, remedy, power, or privilege, nor shall such exercise or any single exercise preclude or impair any further exercise under this clause or the exercise of any other right, power, or privilege of the Government.

(l) Content of Contractor's request for performance-based payment. The Contractor's request for performance-based payment shall contain the following:

(1) The name and address of the Contractor;

(2) The date of the request for performance-based payment;

(3) The contract number and/or other identifier of the contract or order under which the request is made;

(4) Such information and documentation as is required by the contract's description of the basis for payment; and

(5) A certification by a Contractor official authorized to bind the Contractor, as specified in paragraph (m) of this clause.

(m) Content of Contractor's certification. As required in paragraph (l)(5) of this clause, the Contractor shall make the following certification in each request for performance-based payment:

I certify to the best of my knowledge and belief that-

(1) This request for performance-based payment is true and correct; this request (and attachments) has been prepared from the books and records of the Contractor, in accordance with the contract and the instructions of the Contracting Officer;

(2) (Except as reported in writing on _____), all payments to subcontractors and suppliers under this contract have been paid, or will be paid, currently, when due in the ordinary course of business;

(3) There are no encumbrances (except as reported in writing on _____) against the property acquired or produced for, and allocated or properly chargeable to, the contract which would affect or impair the Government's title;

(4) There has been no materially adverse change in the financial condition of the Contractor since the submission by the Contractor to the Government of the most recent written information dated _____; and

(5) After the making of this requested performance-based payment, the amount of all payments for each deliverable item for which performance-based payments have been requested will not exceed any limitation in the contract, and the amount of all payments under the contract will not exceed any limitation in the contract.

(End of clause)

52.247-67 Submission of Transportation Documents for Audit

(a) The Contractor shall submit to the address identified below, for prepayment audit, transportation documents on which the United States will assume freight charges that were paid –

(1) By the Contractor under a cost-reimbursement contract; and

(2) By a first-tier subcontractor under a cost-reimbursement subcontract thereunder.

(b) Cost-reimbursement Contractors shall only submit for audit those bills of lading with freight shipment charges exceeding $100. Bills under $100 shall be retained on-site by the Contractor and made available for on-site audits. This exception only applies to freight shipment bills and is not intended to apply to bills and invoices for any other transportation services.

(c) Contractors shall submit the above referenced transportation documents to—

Contract Officer (CO): Toya Reynolds (Toya.Reynolds@hq.dhs.gov) 202-447-5666

Contract Specialist (CS): Matthew Wetzel (Matthew.Wetzel@hq.dhs.gov) 202-447-0944

Contracting Officer’s Representative (COR): TBD After Award

(End of Clause)

52.252-4 Alterations in Contract (APR 1984)

Portions of this contract are altered as follows:

- TBD After Award

(End of Clause)

3.0 HOMELAND SECURITY ACQUISITION REGULATION (HSAR) CLAUSES

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The full text of a clause may be accessed electronically by the following web address:

https://www.dhs.gov/publication/hsar

HSAR Clauses Incorporated by Reference		
Clause	Title	Date
3052.203-70	Instructions for Contractor Disclosure of Violations.	SEP 2012
3052.204-71	Contractor Employee Access (Alternate I – SEP 2012)	SEP 2012
3052.205-70	Advertisements, Publicizing Awards, and Releases	SEP 2012
3052.215-70	Key Personnel or Facilities.	DEC 2003
3052.216-71	Determination of Award Fee	SEP 2012
3052.216-72	Performance Evaluation Plan	DEC 2003
3052.216-73	Distribution of Award Fee	DEC 2003
3052.222-70	Strikes or Picketing Affecting Timely Completion of the Contract Work.	DEC 2003
3052.222-71	Strikes or Picketing Affecting Access to a DHS Facility	DEC 2003
3052.228-70	Insurance	DEC 2003
3052.242-72	Contracting Officer's Technical Representative	DEC 2003

The following HSAR Clauses are incorporated by full text:

HSAR 3052.204-70 Security Requirements for Unclassified Information Technology Resources (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

HSAR 3052.209-72 Organizational Conflict of Interest (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting is work performed by carriers or telecommunication companies (or prime contractors to carriers or telecommunication companies) in support of the Priority Telecommunication Service program and the

Next General Network (NGN) Priority Service in support of the Emergency Communications Division (ECD).

Potential conflicts include, but are not limited to:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(b) If any such conflict of interest is found to exist, the Contracting Officer may (1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

___ (1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or ___ (2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

(End of Section I)

SECTION J – LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS

Attachment 1 – Cost/Pricing Schedule

Attachment 2 - Deliverables

Attachment 3 – Quality Assurance Surveillance Plan (QASP) Template

Attachment 4 – Government Furnished Property (GFP) / Government Furnished Information (GFI) List

Attachment 5 - Past Performance Questionnaire

Attachment 6 –Performance Requirements Summary

Attachment 7 – Award Fee Plan

Attachment 8 – Reading Room Instructions (Access to GFI During Solicitation Period)

Attachment 9 – Non-Disclosure Agreement (DHS Form 1000-6) – For Access to GFI

(End of Section J)

SECTION K – REPRESENTATION, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS

1.0 FAR CLAUSES INCORPORATED BY REFERENCE:

The following FAR clauses are incorporated by reference:

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.204-16	Commercial and Government Entity Code Reporting	JUL 2016
52.209-7	Information Regarding Responsibility Matters	FEB 2016
52.209-13	Violation of Arms Control Treaties or Agreements—Certification	JUN 2018
52.230-7	Proposal Disclosure—Cost Accounting Practice Changes	APR 2005

2.0 FAR CLAUSES IN FULL TEXT:

FAR 52.204-8 Annual Representations and Certifications

(a)(1) The North American Industry Classification System (NAICS) code for this acquisition is 541512.

(2) The small business size standard is 27.5M.

(3) The small business size standard for a concern which submits an offer in its own name, other than on a construction or service contract, but which proposes to furnish a product which it did not itself manufacture, is 500 employees.

(b)(1) If the provision at 52.204-7, System for Award Management, is included in this solicitation, paragraph (d) of this provision applies.

(2) If the provision at 52.204-7, System for Award Management, is not included in this solicitation, and the Offeror has an active registration in the System for Award Management (SAM), the Offeror may choose to use paragraph (d) of this provision instead of completing the corresponding individual representations and certifications in the solicitation. The Offeror shall indicate which option applies by checking one of the following boxes:

[ ] (i) Paragraph (d) applies.

[}(ii)Paragraph (d) does not apply and the offeror has completed the individual representations and certifications in the solicitation.

(c)(1) The following representations or certifications in SAM are applicable to this solicitation as indicated:

(i) 52.203-2, Certificate of Independent Price Determination. This provision applies to solicitations when a firm-fixed-price contract or fixed-price contract with economic price adjustment is contemplated, unless–

(A) The acquisition is to be made under the simplified acquisition procedures in part 13;

(B) The solicitation is a request for technical proposals under two-step sealed bidding procedures; or

(C) The solicitation is for utility services for which rates are set by law or regulation.

(ii) 52.203-11, Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions. This provision applies to solicitations expected to exceed $150,000.

(iii) 52.203-18, Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements-Representation. This provision applies to all solicitations.

(iv) 52.204-3, Taxpayer Identification. This provision applies to solicitations that do not include the provision at 52.204-7, System for Award Management.

(v) 52.204-5, Women-Owned Business (Other Than Small Business). This provision applies to solicitations that-

(A) Are not set aside for small business concerns;

(B) Exceed the simplified acquisition threshold; and

(C) Are for contracts that will be performed in the United States or its outlying areas.

(vi) 52.209-2, Prohibition on Contracting with Inverted Domestic Corporations-Representation.

(vii) 52.209-5, Certification Regarding Responsibility Matters. This provision applies to solicitations where the contract value is expected to exceed the simplified acquisition threshold.

(viii) 52.209-11, Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law. This provision applies to all solicitations.

(ix) 52.214-14, Place of Performance-Sealed Bidding. This provision applies to invitations for bids except those in which the place of performance is specified by the Government.

(x) 52.215-6, Place of Performance. This provision applies to solicitations unless the place of performance is specified by the Government.

(xi) 52.219-1, Small Business Program Representations (Basic & Alternate I). This provision applies to solicitations when the contract will be performed in the United States or its outlying areas.

(A) The basic provision applies when the solicitations are issued by other than DoD, NASA, and the Coast Guard.

(B) The provision with its Alternate I applies to solicitations issued by DoD, NASA, or the Coast Guard.

(xii) 52.219-2, Equal Low Bids. This provision applies to solicitations when contracting by sealed bidding and the contract will be performed in the United States or its outlying areas.

(xiii) 52.222-22, Previous Contracts and Compliance Reports. This provision applies to solicitations that include the clause at 52.222-26, Equal Opportunity.

(xiv) 52.222-25, Affirmative Action Compliance. This provision applies to solicitations, other than those for construction, when the solicitation includes the clause at 52.222-26, Equal Opportunity.

(xv) 52.222-38, Compliance with Veterans' Employment Reporting Requirements. This provision applies to solicitations when it is anticipated the contract award will exceed the simplified acquisition threshold and the contract is not for acquisition of commercial items.

(xvi) 52.223-1, Biobased Product Certification. This provision applies to solicitations that require the delivery or specify the use of USDA–designated items; or include the clause at 52.223-2, Affirmative Procurement of Biobased Products Under Service and Construction Contracts.

(xvii) 52.223-4, Recovered Material Certification. This provision applies to solicitations that are for, or specify the use of, EPA–designated items.

(xviii) 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals-Representation. This provision applies to solicitations that include the clause at 52.204-7.)

(xix) 52.225-2, Buy American Certificate. This provision applies to solicitations containing the clause at 52.225-1.

(xx) 52.225-4, Buy American-Free Trade Agreements-Israeli Trade Act Certificate. (Basic, Alternates I, II, and III.) This provision applies to solicitations containing the clause at 52.225-3.

(A) If the acquisition value is less than $25,000, the basic provision applies.

(B) If the acquisition value is $25,000 or more but is less than $50,000, the provision with its Alternate I applies.

(C) If the acquisition value is $50,000 or more but is less than$80,317, the provision with its Alternate II applies.

(D) If the acquisition value is$80,317 or more but is less than $100,000, the provision with its Alternate III applies.

(xxi) 52.225-6, Trade Agreements Certificate. This provision applies to solicitations containing the clause at 52.225-5.

(xxii) 52.225-20, Prohibition on Conducting Restricted Business Operations in Sudan-Certification. This provision applies to all solicitations.

(xxiii) 52.225-25, Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran-Representation and Certifications. This provision applies to all solicitations.

(xxiv) 52.226-2, Historically Black College or University and Minority Institution Representation. This provision applies to solicitations for research, studies, supplies, or services of the type normally acquired from higher educational institutions.

(2) The following representations or certifications are applicable as indicated by the Contracting Officer:

(i) 52.204-17, Ownership or Control of Offeror.

(ii) 52.204-20, Predecessor of Offeror.

(iii) 52.222-18, Certification Regarding Knowledge of Child Labor for Listed End Products.

(iv) 52.222-48, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment- Certification.

(v) 52.222-52, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services-Certification.

(vi) 52.223-9, with its Alternate I, Estimate of Percentage of Recovered Material Content for EPA–Designated Products (Alternate I only).

(vii) 52.227-6, Royalty Information.

__ (A) Basic.

__ (B) Alternate I.

(viii) 52.227-15, Representation of Limited Rights Data and Restricted Computer Software.

(d) The offeror has completed the annual representations and certifications electronically via the SAM website accessed through https://www.sam.gov. After reviewing the SAM database information, the offeror verifies by submission of the offer that the representations and certifications currently posted electronically that apply to this solicitation as indicated in paragraph (c) of this provision have been entered or updated within the last 12 months, are current, accurate, complete, and applicable to this solicitation (including the business size standard applicable to the NAICS code referenced for this solicitation), as of the date of this offer and are incorporated in this offer by reference (see FAR 4.1201); except for the changes identified below [offeror to insert changes, identifying change by clause number, title, date]. These amended representation(s) and/or certification(s) are also incorporated in this offer and are current, accurate, and complete as of the date of this offer.

(End of Clause)

FAR 52.230-1 – Cost Accounting Standards Notices and Certification (OCT 2015)

Note: This notice does not apply to small businesses or foreign governments. This notice is in three parts, identified by Roman numerals I through III.

Offerors shall examine each part and provide the requested information in order to determine Cost Accounting Standards (CAS) requirements applicable to any resultant contract.

If the offeror is an educational institution, Part II does not apply unless the contemplated contract will be subject to full or modified CAS coverage pursuant to 48 CFR 9903.201-2(c)(5) or 9903.201-2(c)(6), respectively.

I. Disclosure Statement -- Cost Accounting Practices and Certification

(a) Any contract in excess of $750,000 resulting from this solicitation will be subject to the requirements of the Cost Accounting Standards Board (48 CFR Chapter 99), except for those contracts which are exempt as specified in 48 CFR 9903.201-1.

(b) Any offeror submitting a proposal which, if accepted, will result in a contract subject to the requirements of 48 CFR Chapter 99 must, as a condition of contracting, submit a Disclosure Statement

as required by 48 CFR 9903.202. When required, the Disclosure Statement must be submitted as a part of the offeror's proposal under this solicitation unless the offeror has already submitted a Disclosure Statement disclosing the practices used in connection with the pricing of this proposal. If an applicable Disclosure Statement has already been submitted, the offeror may satisfy the requirement for submission by providing the information requested in paragraph (c) of Part I of this provision.

Caution: In the absence of specific regulations or agreement, a practice disclosed in a Disclosure Statement shall not, by virtue of such disclosure, be deemed to be a proper, approved, or agreed-to practice for pricing proposals or accumulating and reporting contract performance cost data.

(c) Check the appropriate box below:

* (1) Certificate of Concurrent Submission of Disclosure Statement. The offeror hereby certifies that, as a part of the offer, copies of the Disclosure Statement have been submitted as follows:

(i) Original and one copy to the cognizant Administrative Contracting Officer (ACO) or cognizant Federal agency official authorized to act in that capacity (Federal official), as applicable; and

(ii) One copy to the cognizant Federal auditor.

(Disclosure must be on Form No. CASB DS-1 or CASB DS-2, as applicable. Forms may be obtained from the cognizant ACO or Federal official and/or from the loose-leaf version of the Federal Acquisition Regulation.)

Date of Disclosure Statement: _____ Name and Address of Cognizant ACO or Federal Official Where Filed: _____

The offeror further certifies that the practices used in estimating costs in pricing this proposal are consistent with the cost accounting practices disclosed in the Disclosure Statement.

* (2) Certificate of Previously Submitted Disclosure Statement. The offeror hereby certifies that the required Disclosure Statement was filed as follows:

Date of Disclosure Statement: _____ Name and Address of Cognizant ACO or Federal Official Where Filed: _____

The offeror further certifies that the practices used in estimating costs in pricing this proposal are consistent with the cost accounting practices disclosed in the applicable Disclosure Statement.

* (3) Certificate of Monetary Exemption. The offeror hereby certifies that the offeror, together with all divisions, subsidiaries, and affiliates under common control, did not receive net awards of negotiated prime contracts and subcontracts subject to CAS totaling $50 million or more in the cost accounting period immediately preceding the period in which this proposal was submitted. The offeror further certifies that if such status changes before an award resulting from this proposal, the offeror will advise the Contracting Officer immediately.

* (4) Certificate of Interim Exemption. The offeror hereby certifies that

(i) the offeror first exceeded the monetary exemption for disclosure, as defined in (3) of this subsection, in the cost accounting period immediately preceding the period in which this offer was submitted and

(ii) in accordance with 48 CFR 9903.202-1, the offeror is not yet required to submit a Disclosure Statement. The offeror further certifies that if an award resulting from this proposal has not been made within 90 days after the end of that period, the offeror will immediately submit a revised certificate to the Contracting Officer, in the form specified under subparagraph (c)(1) or (c)(2) of Part I of this provision, as appropriate, to verify submission of a completed Disclosure Statement.

Caution: Offerors currently required to disclose because they were awarded a CAS-covered prime contract or subcontract of $50 million or more in the current cost accounting period may not claim this exemption (4). Further, the exemption applies only in connection with proposals submitted before expiration of the 90-day period following the cost accounting period in which the monetary exemption was exceeded.

II. Cost Accounting Standards -- Eligibility for Modified Contract Coverage

If the offeror is eligible to use the modified provisions of 48 CFR 9903.201-2(b) and elects to do so, the offeror shall indicate by checking the box below. Checking the box below shall mean that the resultant contract is subject to the Disclosure and Consistency of Cost Accounting Practices clause in lieu of the Cost Accounting Standards clause.

* The offeror hereby claims an exemption from the Cost Accounting Standards clause under the provisions of 48 CFR 9903.201-2(b) and certifies that the offeror is eligible for use of the Disclosure and Consistency of Cost Accounting Practices clause because during the cost accounting period immediately preceding the period in which this proposal was submitted, the offeror received less than $50 million in awards of CAS-covered prime contracts and subcontracts. The offeror further certifies that if such status changes before an award resulting from this proposal, the offeror will advise the Contracting Officer immediately.

Caution: An offeror may not claim the above eligibility for modified contract coverage if this proposal is expected to result in the award of a CAS-covered contract of $50 million or more or if, during its current cost accounting period, the offeror has been awarded a single CAS-covered prime contract or subcontract of $50 million or more.

III. Additional Cost Accounting Standards Applicable to Existing Contracts

The offeror shall indicate below whether award of the contemplated contract would, in accordance with subparagraph (a)(3) of the Cost Accounting Standards clause, require a change in established cost accounting practices affecting existing contracts and subcontracts.

* yes * no

(End of Provision)

(End of Section K)

SECTION L – INSTRUCTIONS, CONDITIONS, AND NOTICES TO OFFERORS

1.0 GENERAL

The Contractor may submit a proposal for the effort that is identified in Section C of this solicitation. The proposal must be sufficiently detailed and complete to demonstrate an understanding of, and the ability to comply with, all of the requirements in this Request for Proposal (RFP). The proposal should demonstrate such understanding and ability in a concise, logical manner, and shall not contain superfluous material, which is not directly related to this solicitation. General statements, such as that the Offeror can or will comply with requirements, that standard procedures will be used, that well known techniques will be used, or statement that otherwise paraphrase Section C of this RFP, in whole or in part, will not constitute compliance with these requirements concerning the content of the technical proposal.

The proposals shall be submitted electronically to both Matthew Wetzel, Contract Specialist (Matthew.Wetzel@hq.dhs.gov) and Toya Reynolds, Contracting Officer (Toya.Reynolds@hq.dhs.gov) no later than **2:00PM EST Friday May 31st, 2019.**

Any questions regarding this RFP shall be submitted in writing to both Matthew Wetzel, Contract Specialist (Matthew.Wetzel@hq.dhs.gov) and Toya Reynolds, Contracting Officer (Toya.Reynolds@hq.dhs.gov) no later than **2:00PM EST Friday April 26th, 2019.**

To be considered timely, electronic copies of the proposal submission must be received at the specified email address no later than **2:00PM EST Friday May 31st, 2019.** The Government will confirm receipt of your submission via email reply. Quotations not received by the time and date specified and in the manner specified herein will be considered non-responsive and eliminated from further consideration.

Offerors that fail to provide in their initial proposal all information required relative to the submission instructions herein may be found unacceptable and rejected if the Contracting Officer determines that a significant revision or addendum to their proposal would be required to permit further evaluation, and especially if the incomplete proposal appears to be due from a lack of diligence or competence from the Offeror.

Failure to conform to the requirements of the RFP may form the basis of a rejection of the Offeror's proposal.

1.1 Proposal Integrity

In responding to this RFP, it is the Offeror's responsibility to provide current, complete and accurate information in their proposal. If in reviewing the proposal the Government identifies or otherwise learns that the information provided in the proposal is not accurate or misrepresents the Offeror's status or capability, that information may be used by the Contracting Officer as part of the Offeror's responsibility determination and could result in the Offeror not being eligible for award.

1.2 Expenses Related To Offeror Submission

The Government is not responsible for and will not pay or reimburse any costs incurred by the Offeror in the development, submission or any other part of the proposal under this RFP. This includes costs associated with any research, studies, or designs carried out for the purpose of incorporation into any part of the proposal. This also includes any costs to acquire or contract for any services or product relating to the proposal under this RFP.

2.0 PROPOSAL REQUIREMENTS

2.1 General Format Instructions

Contractor shall furnish its proposal in two (2) separate volumes: Volume I: Technical/Management (in PDF or MS Word 2010 Format or higher) and Volume II: Cost/Price Proposal (in MS Excel 2010 Format or higher) as specified below. Each volume shall be complete in itself in order that evaluation of one volume may be accomplished independently of, and concurrently with, evaluation of the other. Individual files sizes shall not exceed 5MB.

The proposal shall be prepared on standard 8 ½" x 11" paper, single-spaced, with 1" minimum margins. The font small be no smaller than 12-point font. Photo-reducing of text is not permitted. Charts, graphs, and tables may be double or single spaced and are included in the 35-page count limit in the technical proposal. Header/footer information (which does not include any information to be evaluated) may be included in the 1" margin space. Tabs do not count against page restrictions. Proposal shall not exceed the page limitations set forth below. Pages that exceed the maximum page limitation will not be evaluated.

2.2 Format and Instructions for Proposal Submission

Proposal shall consist of the following two (2) separate volumes with the maximum number of pages for each proposal Volume as listed below. Each volume shall be a separate electronic file. Please note that any pages exceeding the maximum pages state in the instructions below will not be evaluated by the Government.

In order for the technical proposal to be evaluated strictly on the merit of the material submitted, NO PRICE INFORMATION IS TO BE INCLUDED IN VOLUME I. Each volume shall be separate and complete in itself so that evaluation of one may be accomplished independently from the evaluation of the other.

VOLUME I: TECHNICAL/MANAGEMENT PROPOSAL:

The Technical/Management Volume shall not exceed 35 pages, excluding the Quality Assurance Surveillance Plan (QASP), Performance Requirements Summary, resumes of Key Personnel, past performance citations, cover letter, title page and table of contents. Each resume shall not exceed three (3) pages. The cover letter and title page shall not exceed one (1) page each. The table of contents shall not exceed two (2) pages. Past performance citations shall not exceed (2) pages each. The Offeror shall demonstrate an understanding of the requirement and ability to successfully to perform the effort as stated herein by addressing the evaluation factors below.

Volume I shall consist of the following tabs:

TAB A – Cover Letter and Title Page (One (1) Page Each)

A cover letter shall accompany the proposal to set forth any information that the Offeror wishes to bring to the attention of the Government. The cover letter shall also stipulate that the Offeror's proposal is predicated upon all the terms and conditions of this RFP. In addition, it must contain a statement that the Offeror's acceptance period is valid for at least ninety (90) calendar days from the date of receipt by the Government.

All proposal submissions must include the following information in the cover letter:

- Dun & Bradstreet Number (DUNS)
- North American Industrial Classification Systems (NAICS) Code
- Standard Product Code
- Contact Name, Email, Telephone, and Fax Number
- Complete Business Mailing Address
- CAGE Code (If Applicable)

TAB B – Table of Contents (No More Than Two (2) Pages)

TAB C – Technical Evaluation Factors (Not To Exceed 35 Pages)

The Offeror's technical submission shall demonstrate the firm's capability to perform the requirements outlined in the RFP. Offerors shall provide a technical proposal that addresses the following three (3) factors:

- Technical Approach and Understanding
- Management Approach and Capabilities
- Past Performance

Factor 1: Technical Approach and Understanding

The Offeror must define their Technical Approach and Understanding that satisfies the requirements defined in the Performance Work Statement (PWS). The Offeror's Technical Approach and Understanding should include the following:

• Discussion of the background, objectives and work requirements of the PWS;

• Discussion of the proposed methods and techniques for completing each task;

• Discussion which supports how each task will be evaluated for full performance and acceptability of work from the Offeror's perspective;

• Discussion of any anticipated major difficulties and problem areas, along with potential recommended approaches for their resolution; and

• Discussion of major logistical considerations.

Technical Proposals shall address the following elements (all of the same, equal importance):

Element 1 – Local Exchange Carrier and Wireless Services

The Offeror must address the approach to sustain Government Emergency Telecommunications Services (GETS), Special Routing Arrangement Service (SRAS), and Wireless Priority Services (WPS), the requisite service engineering and contracting to maintain GETS/SRAS priority features and functions within selected local exchange carriers (LEC) networks and the requisite WPS service engineering and contracting support to maintain priority features and functions within wireless carrier networks. Planning concerning tariff and other contract arrangements must be fully explained to include GETS/WPS Carrier Agreements for the Base Year and all Option Periods. A sample LEC and WPS subcontract shall be provided by the Offerors for evaluation.

Element 2 – Engineering Support

The Offeror must demonstrate an understanding of the scope and complexity of extending the service viability for GETS, GETS VoIP, WPS, and WPS VoLTE. Specifically, Offerors must describe their approach to providing the requisite service engineering to ensure that schedule, cost and performance goals are met.

The Offeror must describe their capabilities involving correction of service performance problems and/or service degradation of GETS, SRAS, and WPS including the requisite planning, design, engineering, procurement, testing, and implementation/deployment of technology or network upgrades and/or fixes.

The Offeror must address Sustainment Engineering Objective to provide the requisite engineering to extend the service viability for GETS and WPS while ensuring that these services support user requirements in a manner that protects National Security/ Emergency Preparedness (NS/EP) equities; and address their capability to support Future Services Engineering Objectives to provide the requisite engineering to plan for NGN PTS for follow-on NGN GETS and WPS.

Element 3 – Operational Support

The Offeror must describe the approach to support analysis of GETS, GETS VoIP, SRAS WPS, and WPS VoLTE performance to meet objectives for intra/interagency emergency communications, international interface, interoperability, nationwide coverage, survivability/endurability, and voice-band service. This element shall also concentrate on the readiness capabilities as stated in the PWS. The Offeror shall explain how it will use innovative methods to improve operations, administration and maintenance (OA&M) application methods and processes and how it will ensure that the network operation center works with carrier operations centers to identify, coordinate, and correct network service problems. All proposed operations, administration, maintenance, and provisioning (OAM&P) areas must be explained in the defined approach. This element shall also concentrate on the Security, Improved Operational Support, Enhanced Service Performance Metrics, and Carrier Support objectives of the PWS.

Element 4 – Testing Support

The Offeror must demonstrate an understanding of GETS, GETS VoIP, SRAS, WPS, and WPS VoLTE requirements as well as the procedures and processes in testing traffic and signaling call flow and understanding of and experiences with network metrics and Key Performance Parameters (KPPs). The proposal must reflect the understanding of network and laboratory equipment uses with the most

current IP capabilities being used in large scale telecommunications networks. The Offeror must demonstrate the understanding, the implementation and the operations of WPS on Voice over LTE (VoLTE). The Offeror must demonstrate the understanding of test development and analysis and reporting of network problems affecting flow and delivery of priority emergency traffic. Specifically, the Offeror must have demonstrated experience in performing reoccurring operational testing, Network Service Verification Test (NSVT), Captive Office Test (COT), and Networks Services Acceptance Test (NSAT).

Element 5 – Transition Services

The Offeror shall fully define the approach to transition for Contract Phase-In and Phase-Out as stated in the PWS.

Element 6 –Service Center

The Offeror shall address Service Center objectives as stated in the PWS.

Element 7 - Technology Refresh

The Offeror shall address Technology Refreshment objectives as stated in the PWS.

Element 8 – Quality Assurance Surveillance Plan (QASP)

The Offeror shall prepare a draft Quality Assurance Surveillance Plan (QASP) using the template provided (Attachment 3) which provides systematic Quality Assurance methods to be use in the administration of the Performance Based Service Contract (PBSC) standards included in this contract. As part of the QASP, the Offeror shall also prepare a Performance Requirements Summary (PRS) matrix using the template provide (Attachment 6) listing all readiness and non-readiness requirements of the PWS. The intent is to ensure that the Contractor performance in accordance with performance metrics set forth in the Performance Requirements Summary (PRS) that the Government receives the quality of services called for in the contract and that the Government only pays for the acceptable level of services received. The Government is not obligated to use this document. However, if accepted, the QASP becomes a Government document and the Government retains the responsibility for execution of the document. The Offeror-prepared QASP shall contain recommendations on the Acceptable Quality Level (AQL) associated with requirements and performance standards.

Factor 2: Management Approach and Capabilities

The Offeror's management approach and capabilities shall include information that is simple, easy to read and clearly describes project personnel and responsibilities, any proposed subcontracting arrangements, communication and coordination plans, schedules of all tasks and subtasks, meetings, and deliverables.

The Offeror's management approach shall include the company's contingency and continuity of operations plans in the event of a natural or manmade disaster that may disrupt service capabilities.

The Offeror's management approach shall include all key and non-key personnel and a description of the firm's current personnel resources. The Offeror's labor mix required to conduct the tasks and produce any deliverables must be identified. The personnel portion of the Offeror's proposal shall include:

A. Resumes of proposed Key Personnel are required. Resumes are limited to three (3) pages and shall indicate the proposed job category that the individual will perform. The resumes shall contain at a minimum: company name/address; telephone number; points of contact; duties performed by individual Key Personnel; dates employed; qualifications; experience and capability; skills; accomplishments; availability; and credentials (education, training, and certifications). Show the knowledge that the personnel have gained through completed and ongoing efforts that are similar in nature to this effort.

B. The Government will assess the qualifications of proposed key personnel and availability of the proposed project staff. The evaluation will include an assessment of the strengths, weakness, and risks associated with the qualifications and experience of the proposed key personnel.

Key Personnel Qualifications are as follows:
• Program Manager
• Sustainment Engineering Lead
• WPS Lead
• OAM&P Lead
See Section H, Item 16.3 “Key Personnel” for Key Personnel minimum qualifications guidelines.

Factor 3: Past Performance

The Offeror shall identify three (3) of its most recent contracts (Federal, State, local government, and/or private), either completed or still ongoing within the past three (3) years of the date of this RFP, that demonstrate successful execution of the same or similar services as those contained in the PWS. Furthermore, Offeror’s shall include a list of all relevant DHS on-going contracts or contracts completed for the specified period. Each past performance citation may not exceed two (2) pages. For each past performance citation identify the following information:

1) Project Title
2) Description of the Project
3) Contract/Task Order Number
4) Contract/Task Order Total Amount
5) Government Agency/Organization
6) COR’s Name, Address, Telephone Number, and Email Address
7) Current Status (i.e. Completed, In-Progress / Estimated Start and Completion Dates)
8) A Brief Narrative of Why Offeror Believes this Reference is Relevant to the Proposed Contract

Past Performance references shall be a prime Contractor or first-tier subcontractor on previous or current projects/tasks that are similar in size, scope, and complexity to work identified in the PWS. Past Performance does not necessarily have to be Government-related; but it is important to demonstrate and provide evidence of past performance for work **similar in size, scope and complexity.**

Offerors shall forward the Past Performance Questionnaire (Attachment 5) to the Offeror’s references. The references shall forward their completed questionnaires to the Contract Specialist (Matthew.Wetzel@hq.dhs.gov) NOT BACK TO THE OFFEROR no later than May 31, 2019 at 2PM EST. Any questionnaire received after the designated time and date will NOT be considered.

VOLUME II: COST/PRICE PROPOSAL:

(NOTICE TO OFFERORS: IT IS IMPERATIVE THAT OFFERORS ADHERE TO THE COST/PRICE PROPOSAL INSTRUCTION SET FORTH BELOW. FAILURE TO COMPLY WITH THE INSTRUCTIONS MAY RESULT IN THE REJECTION OF THE PROPOSAL BY THE GOVERNMENT)

Volume II shall consist of the following Tabs:

TAB A – Exceptions and Deviations

Each proposal shall include an exceptions/deviations section in Volume II that identifies and explains in detail any exceptions, deviations, or conditional assumptions taken with the requirements of the RFP. Any exception, etc. taken must contain sufficient amplification and justification to permit evaluation. All benefits to the Government shall be fully explained for each exception taken. Such exceptions will not, of themselves, automatically cause a proposal to be deemed unacceptable. A large number of exceptions, or one or more significant exceptions not providing benefit to the Government, may however, result in rejection of the Offeror's proposal as unacceptable.

TAB B – Contract Documents and Associated Information

The Offeror shall provide a completed and signed copy of the Standard Form (SF) 33, and any SF-30s (Amendments).

In Offeror's proposal, Offeror must certify that Offeror is not an "inverted domestic corporation" as defined in FAR 52.209-2 Prohibition on Contracting with Inverted Domestic Corporations - Representation (NOV 2016) and certify there is no organizational conflict as defined in HSAR Clause 3052.209-72, Organizational Conflict of Interest (OCI) (JUN 2006) paragraph (c) of the Homeland Security Acquisition Regulation (HSAR).

The Offeror shall also include a statement regarding Online System for Award Management (SAM) submission.

TAB C – Price/Cost Proposal

The Cost/Price Proposal shall include the following information:

1) Completed Cost/Price Schedule (Attachment 1) for this Contract

Offerors shall submit a proposal on a hybrid basis with specific CLINS reflecting Firm-Fixed-Price (FFP), Cost-Plus-Award-Fee (CPAF), and Cost Reimbursable (CR) (i.e. unburdened direct labor rates, indirect rates, and other direct costs, fee and fee percentage) the provides the Offeror's labor categories and corresponding labor hours to satisfy the requirements of the base and option periods included herein. It must also identify any Government Furnished Equipment (GPE) or Government Furnished Information (GFI) requires for the contract performance.

Offerors must adhere to the Key Personnel labor categories and minimum qualifications prescribed herein and on the Cost/Price Schedule (Attachment 1) in their proposal, however the offeror may propose other and additional labor categories for all non-key personnel using their own business acumen and judgement in order to successfully perform the required task(s). The offeror shall provide a total cost summary with major cost elements along with a detailed breakdown of each task that

identifies the labor categories proposed, hourly rates for Contractor site and the total number of hours proposed for each labor category for each period of performance. Cost supporting details shall include base labor rates, fringe benefits, overhead, General and Administrative (G&A) expenses, Other Direct Costs, indirect rates, and calculation methodology. The sum total of the CLIN breakdown shall equal the CLIN price. Identify the proposed key personnel and their corresponding labor category. (This information must be included in a separate Microsoft Excel Document). The supporting details shall include Offeror's Forward Pricing Rate Agreements (FPRAs), identification of cognizant audit agency with point of contact's name, email address, and telephone number, include the approval Memorandums from DCAA/DCMA validating the adequacy of Offeror's accounting system and disclosure statement prior to award.

Offerors must fully explain and document the derivation of direct and indirect rates. All direct and indirect rates proposed are subject to DCAA verification. The proposal shall also identify any price reductions or discounts offered.

The Government has provided an estimated travel, and other direct costs (ODCs), for this contract. This amount has been inserted into the Cost/Pricing Schedule (Attachment 1) and will serve as the evaluated cost during each period of performance under this contract. If an Offeror intends to recover indirect costs on travel, during the contract's performance period, the Cost Volume Quotation shall include a narrative statement which identifies the rate to be utilized and the supporting documentation included with the proposal to substantiate the rate. The application of any proposed indirect rates must be consistent with the Offeror's normal business practices. The requirement for a narrative statement does not require the calculation of travel costs, or Other Direct Costs. (Note: No profit or fee shall be applied to these areas).

Please note, the cost/price data provided in Offeror's proposal must price the effort for one (1) one-year base period of performance and four (4) one-year option periods. (For pricing purposes, assume that the initial period of performance will be on or about August 17, 2019 through August 16, 2024). Price the proposal by option period, labor category, and by number of hours per labor category (Attachment 1). Labor categories shall correspond to those provided in the staffing matrix that should also be included in the cost/price detail. All cost/price data shall be provided in Microsoft Excel (version 2010 or higher) with the formulas included in the worksheets. The Offeror's cost/price data must result in clearly identifiable costs/prices (for the one (1) one-year base and four (4) one-year option periods) for the number of hours proposed as well as clearly identifiable costs/prices for the entire requirement.

3.0 FAR CLAUSES

The following FAR clauses are incorporated by reference:

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.204-7	System of Award Management	OCT 2016
52.207-1	Notice of Standard Competition	MAY 2006
52.214-34	Submission of Offers in the English Language	APR 1991
52.214-35	Submission of Offers in U.S. Currency	APR 1991
52.215-1	Instructions to Offerors—Competitive Acquisition	OCT 1997

52.215-20	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data	OCT 2010
52.215-22	Limitations on Pass-Through Charges—Identification of Subcontract Effort	OCT 2009
52.237-10	Identification of Uncompensated Overtime	MAR 2015

The following FAR Clauses are incorporate using full text:

FAR 52.216-1 Type of Contract (APR 1984)

The Government contemplates award of a hybrid contract resulting from this solicitation using a combination of Firm-Fixed-Price (FFP), Cost Reimbursement (CR) and Cost-Plus-Award-Fee (CPAF) CLINS.

FAR 52.233-2 Service of Protest (SEP 2006)

(a) Protests, as defined in section 33.101 of the Federal Acquisition Regulation, that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), shall be served on the Contracting Officer by obtaining written and dated acknowledgment of receipt from the Contracting Officer.

(b) The copy of any protest shall be received in the office designated above within one day of filing a protest with the GAO.

(End of Section L)

SECTION M – EVALUATION FACTORS FOR AWARD

1.0 GENERAL

A single award will be made to the responsible Offeror submitting an overall proposal that is determined most advantageous to the Government, cost/price and non-cost/price factors considered. Award will be made to the Offeror whose proposal meets the Government's requirements and whose technical proposal and cost/price represent the best value to the Government. The evaluation of proposals will be based on the following factors:

Technical Approach and Understanding
Management Approach and Capabilities
Past Performance
Cost/Price

The relative order of importance of the evaluations factors are as follows: Factor 1 (Technical Approach and Understanding) is more important than Factor 2 (Management Approach and Capabilities) which is more important than Factor 3 (Past Performance), and each factor is individually more important than Factor 4 (Cost/Price); and when combined, non-cost/priced factors are significantly more important than Cost/Price.

In the event that two or more proposal are determined to be technically equivalent, cost/price will become more important, and award may be made to the lower priced Offeror. It should be noted that award may be made to other than the lowest priced proposal if the Government determines that a price premium is warranted due to technical merit. The Government may also award to other than the highest technically rated proposal, if the Government determines that a price premium is not warranted.

The Government intends to evaluate offers and award a single contract without discussions with Offerors. Therefore, the Offeror's initial offer should contain the best terms from a cost/price and technical standpoint. However, the Government reserves the right to conduct discussions with all Offerors. If discussions are conducted, Offerors will be given an opportunity to submit a final revised proposal to the Government if necessary.

2.0 EVALUATION FACTORS

Factor 1: Technical Approach and Understanding

The Government will evaluate the Offeror's technical approach and demonstrated understanding of the requirements necessary to accomplish the work outlined herein. In conducting the evaluation, the Government will be seeking to determine the overall extent to which the Offeror fully understands and has experience with the technical requirements and demonstrates understanding with the following (all of the same, equal importance) :

Element 1 – Local Exchange Carrier and Wireless Services - Knowledge and approach to sustain Government Emergency Telecommunications Services (GETS), Special Routing Arrangement Service (SRAS), and Wireless Priority Services (WPS), the requisite service engineering and contracting to

maintain GETS/SRAS priority features and functions within selected local exchange carriers (LEC) networks and the requisite WPS service engineering and contracting support to maintain priority features and functions within wireless carrier networks. Planning concerning tariff and other contract arrangements must be fully explained to include GETS/WPS Carrier Agreements as well as provided sample of LEC and WPS subcontracts for evaluation.

Element 2 – Engineering Support – Thorough understanding of the scope and complexity of extending the service viability for GETS, GETS VoIP, WPS, and WPS VoLTE. Specifically, the approach to providing the requisite service engineering to ensure that schedule, cost and performance goals are met. Also the capabilities involving correction of service performance problems and/or service degradation of GETS, SRAS, and WPS including the requisite planning, design, engineering, procurement, testing, and implementation/deployment of technology or network upgrades and/or fixes. Addressing the Sustainment Engineering Objective to provide the requisite engineering to extend the service viability for GETS and WPS while ensuring that these services support user requirements in a manner that protects National Security/ Emergency Preparedness (NS/EP) equities; and address their capability to support Future Services Engineering Objectives to provide the requisite engineering to plan for NGN PTS for follow-on NGN GETS and WPS.

Element 3 – Operational Support The approach to support analysis of GETS, GETS VoIP, SRAS WPS, and WPS VoLTE performance to meet objectives for intra/interagency emergency communications, international interface, interoperability, nationwide coverage, survivability/endurability, and voice-band service. This element shall also concentrate on the readiness capabilities as stated in the PWS. Explanation of how the offeror will use innovative methods to improve operations, administration and maintenance (OA&M) application methods and processes and how it will ensure that the network operation center works with carrier operations centers to identify, coordinate, and correct network service problems. All proposed operations, administration, maintenance, and provisioning (OAM&P) areas must be explained in the defined approach. Also concentrate on the Security, Improved Operational Support, Enhanced Service Performance Metrics, and Carrier Support objectives of the PWS.

Element 4 – Testing Support - Understanding of GETS, GETS VoIP, SRAS, WPS, and WPS VoLTE requirements as well as the procedures and processes in testing traffic and signaling call flow and understanding of and experiences with network metrics and Key Performance Parameters (KPPs). The proposal must reflect the understanding of network and laboratory equipment uses with the most current IP capabilities being used in large scale telecommunications networks. The Offeror must demonstrate the understanding, the implementation and the operations of WPS on Voice over LTE (VoLTE). The Offeror must demonstrate the understanding of test development and analysis and reporting of network problems affecting flow and delivery of priority emergency traffic. Specifically, the Offeror must have experience in performing reoccurring operational testing, Network Service Verification Test (NSVT), Captive Office Test (COT), and Networks Services Acceptance Test (NSAT).

Element 5 – Transition Services - The approach for a successful and sound transition for Contract Phase-In and Phase-Out as stated in the PWS.

Element 6 –Service Center- The approach and demonstrated understanding to address Service Center objectives as stated in the PWS.

Element 7 - Technology Refresh **-** Approach and demonstrated understanding to address Technology Refreshment objectives as stated in the PWS.

Element 8 – Quality Assurance Surveillance Plan (QASP) – Sound and reasonable QASP in order to provide systematic Quality Assurance methods to be use in the administration of the Performance Based Service Contract (PBSC) standards included in this contract. As part of the QASP, the Government will evaluated the Performance Requirements Summary (PRS) listing all readiness and non-readiness requirements of the PWS. The intent is to ensure that the Contractor performance in accordance with performance metrics set forth in the Performance Requirements Summary (PRS) that the Government receives the quality of services called for in the contract and that the Government only pays for the acceptable level of services received. QASP shall contain recommendations on the Acceptable Quality Level (AQL) associated with requirements and performance standards.

Additionally, the appropriateness, soundness and reasonableness of the Offeror's problem resolution approach and logistic consideration will be evaluated.

Factor 2: Management Approach and Capabilities

The Government will evaluate the extent to which the Quoter's management approach and capabilities demonstrates sound and reasonable business practices with respect to effectively managing the requirements of the PWS in terms of management and business capabilities, project personnel and responsibilities, any proposed subcontracting arrangements, communication and coordination plans, schedules of all tasks and subtasks, meetings, and deliverables.

The Government will evaluate the Offeror's contingency and continuity of operations plans for soundness and effectiveness in the event of a natural or manmade disaster that may disrupt service capabilities.

The Government will assess the qualifications of key personnel and availability of the proposed non-key personnel staffing, including consultants and subcontractors. The evaluation will include an assessment of the strengths, weaknesses, and risks associated with the qualifications and experience of the proposed key personnel and labor mix.

Factor 3: Past Performance

The Government will assess the relevance, breadth and quality of the Offeror's recent past performance on similar type of work. The Government will evaluated the quality of the Offeror's past performance based on the past performance reference provided in the Offeror's proposal and/or other information obtained from references provided by the Offeror, as well as other relevant past performance information obtained from other sources known to the Government. The Government reserves the right to perform customer surveys only from those contracts which are deemed by the Government to be the most relevant to this procurement. An Offeror without a record of past performance or for whom information on relevant past performance is not available will be evaluated as neutral.

The Government reserves the right to use publicly available reports and data retrieved from the Contract Performance Assessment Reporting System (CPARS) and any other present and/or past performance data obtained from a variety of sources; not just those contract identified by Offerors. Past performance citations will be assessed by Government through CPARS at http://www.cpars.gov

Factor 4: Cost/Price

While not a rated factor, cost/price to the Government will be a factor in selecting the successful Offeror. Cost/Price will be evaluated with respect to completeness, and reasonableness based on the information submitted in the Offeror's Cost/Price Proposal (Volume II). Cost realism analyses shall only be performed on Cost Reimbursable (CR) and Cost-Plus-Award-Fees (CPAF) CLINs (with the exception of Optional CLINs X011 – Technology Refreshment). In the event the Government exercises Optional CLINs X011, the Government will determine at that time whether the costs for those CLINs are realistic.

The cost/price proposal will be evaluated to determine whether costs/prices are realistic only with regard to the Cost Reimbursable (CR) and Cost-Plus Award Fee (CPAF) CLINs for any resultant work to be performed, reflect a clear understanding of the requirements, and are consistent with the approaches described in the technical proposal.

Firm-Fixed-Price (FFP) CLINs will be verified using other than certified cost and pricing data. Price Competition is expected for this requirement

The evaluation of the Offeror's cost/price proposal will consider the following:

1) Completeness

The cost/price proposal will be evaluated as to completeness, including the adequacy of supporting data.

2) Reasonableness

The cost/price proposal will be evaluated for reasonableness of the overall cost/price by comparing to the other submitted competitive proposals or the Independent Government Cost Estimated (IGCE) if necessary. The evaluation will determine if cost/price included in the Offeror's proposal is reasonable given the nature of the work to be performed and the supporting explanations and information provided.

The options proposed in accordance with the RFP will be evaluated in the same manner as the base award. The Government will evaluate the Offeror's cost/price proposal for award purposes by adding the total cost/price for the options to the cost/price for the base requirement.

Evaluation of options does not obligate the Government to exercise the options. The Government reserves the right to exercise some, all or none of the option and optional CLINs.

3.0 BASIS OF AWARD

The Government will award a contract to the responsible Contractor whose proposal is determined most advantageous to the Government, cost/price and non-cost/price factors considered. The Offeror's proposal will be evaluated for compliance with terms, conditions and requirement set forth by the solicitation. All non-cost/price factors, when combined, are significantly more important than price/cost.

4.0 FAR CLAUSES

FAR Clauses Incorporated by Reference		
Clause	Title	Date
52.217-5	Evaluation of Options	JUL 1990

(End of Section M)